small_frog/E+/Getty Images

Cross-Border Discovery Under the GDPR

The recently enacted General Data Protection Regulation (GDPR) poses significant challenges for organizations with an international reach, particularly in the context of discovery for US disputes, and carries potentially massive monetary penalties for non-compliance. While there is uncertainty about how some GDPR provisions will be interpreted and enforced in practice, organizations and their counsel should take proactive steps to understand the new regulation and implement best practices for navigating cross-border discovery.

DAVID R. COHEN
PARTNER
REED SMITH LLP

David is chair of the firm's Records & E-Discovery (RED) Group and has more than 30 years of commercial litigation experience in a variety of subject matters. He serves as special e-discovery counsel in many cases, represents companies in complex litigation matters, and counsels clients on records management and litigation readiness issues.

ERICA YEN
ASSOCIATE
REED SMITH LLP

Erica is a member of the firm's Life Sciences Health Industry Group and an ambassador member of the RED Group. She focuses her practice on products liability litigation, representing pharmaceutical and medical device clients in state and federal courts. Erica also counsels clients on e-discovery issues.

The much anticipated GDPR (Regulation (EU) 2016/679), which governs the processing of personal data of individuals in the European Union (EU), became effective on May 25, 2018. The GDPR was incorporated by the European Economic Area (EEA) Joint Committee into the EEA Agreement on July 6, 2018, making it applicable to Iceland, Norway, and Liechtenstein as well as to the 28 EU member states.

The new regulation supersedes the 1995 EU Data Protection Directive (95/46/EC) and represents a codified version of the fundamental right to privacy in the EU in a way that differs significantly from the way US law protects personal data. It includes several new provisions to protect the rights of individuals in the EU (referred to as data subjects) and authorizes severe consequences for non-compliance. GDPR violators are subject to penalties of up to the larger of EUR20 million or 4% of an organization's annual global gross revenue. While maximum fines may rarely be imposed, a penalty

of even a fraction of the highest potential amount could have a crippling impact on many organizations.

Any organization that operates in the EU or has EU employees, customers, or clients must put mechanisms in place to protect personal data and maximize compliance with the GDPR. However, these efforts may sometimes conflict with US discovery demands. A litigant may face sanctions for either violating the GDPR or failing to fulfill its US discovery obligations. To minimize risk, organizations and their counsel should:

- Understand the tension between the broad scope of the GDPR and the broad scope of US discovery.
- Review the GDPR requirements impacting US investigations and litigations.
- Implement best practices for navigating cross-border discovery.

GDPR COMPLIANCE VERSUS US DISCOVERY OBLIGATIONS

The GDPR has a broad territorial reach. It applies to organizations acting as data controllers or data processors that are:

- Established in the EU.
- Established in a jurisdiction where EU member state law applies through public international law.
- Not established in the EU but either:
  - offer goods or services to data subjects in the EU; or
  - monitor the behavior of data subjects in the EU.

(GDPR, Article 3.)

The GDPR imposes restrictions on processing, transferring, and retaining personal data, and broadly defines both "personal data" and "processing." Personal data includes "any information relating to an identified or identifiable natural person" (GDPR, Article 4(1)). This definition reflects a significantly broader concept of personal data or personally identifiable information than what is recognized in the US. Any data point that allows a person to be identified (such as an individual's name, an email address, or even a job title and employer's name) constitutes personal data under the GDPR.

The term processing includes "any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available ... erasure or destruction" (GDPR, Article 4(2)).

Information exchanges in US investigations and litigations typically entail the preservation, collection, filtering, review, and production of voluminous quantities of data, much of which includes processing personal data under the GDPR definition. The frequency and amount of disclosure commonly required in US dispute resolution is unfamiliar to most EU privacy officials given that, outside of the UK, the dispute resolution systems in most EU jurisdictions contemplate little (if any) party-driven discovery. Moreover, EU countries tend to give much greater weight to personal privacy because it is a fundamental right in the EU (see Charter of Fundamental Rights of the European Union, Title II, Article 8).

However, US courts often afford little deference to non-US privacy laws when parties object to cross-border discovery. The most pertinent guidance from the US Supreme Court came 30 years ago in *Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa*. In that case, the Court set out factors for lower courts to apply when addressing a request for discovery that implicates foreign law (482 U.S. 522, 546 & n.30 (1987)). Most courts applying those factors have held that the US discovery interests outweighed the EU privacy interests (see, for example, *Knight Capital Partners Corp. v. Henkel Ag & Co., KGaA*, 290 F. Supp. 3d 681, 687 (E.D. Mich. 2017)). Accordingly, it is challenging for organizations with an international reach to comply with US discovery obligations without violating the GDPR.

Search Conflicts Between US Discovery and Non-US Data Protection Laws for more on typical conflicts that can arise between US discovery laws and non-US data protection laws that limit the collection, processing, and cross-border transfer of personal information.

The frequency and amount of disclosure commonly required in US dispute resolution is unfamiliar to most EU privacy officials given that the dispute resolution systems in most EU jurisdictions contemplate little (if any) party-driven discovery. Moreover, EU countries tend to give much greater weight to personal privacy.

KEY GDPR REQUIREMENTS

To maximize compliance with the GDPR when confronted with US discovery obligations, counsel must understand the GDPR requirements that address how an organization:

- Processes personal data.
- Transfers personal data.
- Retains personal data.

Because GDPR compliance is complicated, counsel should consider consulting with knowledgeable local counsel before processing, transferring, or retaining any personal data for a US dispute.

PROCESSING PERSONAL DATA

The GDPR restricts the processing of personal data by an organization in several ways. First, an organization must have a lawful basis for processing the data. The most likely lawful bases for processing personal data for US dispute resolution include where:

- The data subject consents to the processing of her personal data for one or more specific purposes.
- Processing the personal data is necessary to:
  - comply with a data controller's legal obligation under EU state law; or
  - serve a data controller's or a third party's legitimate interests, except where a data subject's fundamental rights and freedoms requiring the protection of her personal data override those legitimate interests.

(GDPR, Article 6(1)(a)-(f).)

Consent

US counsel seeking personal data for a US dispute may try to obtain a data subject's consent to process data for discovery. Consent under the GDPR is a high threshold to meet and maintain, so it is usually not prudent to rely on that basis.

Valid consent must be:

- **Demonstrable.** A data controller bears the burden of proving that it obtained the data subject's consent to process her personal data, typically through a written statement, a ticked box, or a verbal representation (GDPR, Recital 32 ("Silence, pre-ticked boxes or inactivity should not ... constitute consent.")). A data controller's request for consent must be clearly distinguishable from other matters addressed in the request and must be conveyed in clear, plain language.
- **Revocable.** A data subject may freely withdraw consent (GDPR, Article 7(3) ("It shall be as easy to withdraw as to give consent.")). Obtaining revocable consent may be impractical in US disputes because a data controller typically loses control of data once it is produced to another party. However, the GDPR also states that a revocation of consent does not render unlawful any processing performed before the revocation. Organizations that have produced processed personal data based on consent before it was withdrawn may still comply with the GDPR.
- **Voluntary.** A data subject must freely give consent. However, the Article 29 Working Party acknowledged the difficulty associated with determining and establishing that an employee's consent is truly voluntary where it was provided in response to an employer's request.

(GDPR, Article 7; Recitals 32, 33, 42, and 43.)

In addition to these requirements, consent-based processing covers only the consenting data subject's personal data. Because any individual custodian's data will include personal data about numerous other data subjects, securing the consent of every data subject identified in every document, communication, or piece of data is unrealistic in most cases.

Search Consent to Process and Transfer Personal Data in US Discovery for a sample consent form that counsel can use to obtain a data subject's consent to process and transfer personal data protected by non-US data protection laws for production in US discovery, with explanatory notes and drafting tips.

Legitimate Interests

Given the difficulties associated with securing valid consent, parties in US disputes typically rely on the legitimate interests basis to justify processing personal data.

To make the required showing, a litigant must be prepared to demonstrate that the interests or fundamental rights and freedoms of the data subjects do not override the litigant's legitimate interests. Counsel can employ various techniques, including data minimization and protection, to help satisfy that balancing test (see below *Best Practices for Cross-Border Discovery*).

However, a data controller may not invoke the legitimate interests basis to process personal data if the data falls within one of the "special categories" of personal data set by the GDPR, such as:

- Data revealing a data subject's:
  - racial or ethnic origin;
  - political opinions;
  - religious or philosophical beliefs; or
  - trade union membership.
- Genetic data, biometric data, or data concerning health.
- Data concerning a data subject's sex life or sexual orientation.

(GDPR, Article 9(1).)

A data controller may process this type of personal data only if it either:

- Secures the data subject's explicit consent for processing, which is subject to more exacting consent requirements than those identified above (GDPR, Article 9(2)(a); see above *Consent*). Explicit consent requires a data subject to state her consent clearly and in detail, leaving no room for confusion or doubt. Explicit consent can be confirmed expressly through a written statement alone and it can be further bolstered by having the data subject sign the written statement manually

or digitally, fill out an electronic form, or send an email (see Article 29 Working Party, WP 259).

- Demonstrates that the processing is necessary to establish, exercise, or defend legal claims, or that a court is acting in its judicial capacity (GDPR, Article 9(2)(f)).

The GDPR does not explicitly state whether the phrase "legal claims" extends to US legal claims. Accordingly, in the context of cross-border discovery, a data controller should attempt to filter out the special categories of personal data from any further processing or transfers. Even if a party establishes a legal basis to process special categories of personal data for a US dispute, it must also conduct a data protection impact assessment (DPIA) if it intends to process the data on a large scale (see GDPR, Article 35(3); Article 29 Working Party, WP 248).

A DPIA is required where data processing "is likely to result in a high risk to the rights and freedoms of natural persons" (GDPR, Article 35(1); Article 29 Working Party, WP 248 (listing nine criteria to be considered in determining potential "high risk")). A DPIA:

- Describes the nature, scope, context, and purposes of the processing.
- Assesses whether the processing is necessary and proportional.
- Identifies and evaluates risks to data subjects.
- Specifies measures an organization can take to address data risks and demonstrate compliance.

(See GDPR, Article 35(3); Article 29 Working Party, WP 248.)

The DPIA must be continuously updated and overseen by the controller in conjunction with the data protection officer. A DPIA is required in any instance where processing involves risks to the rights and freedoms of natural persons.

If the data controller determines that processing is not likely to result in a high risk, the controller should document the reasons for not carrying out a DPIA. Even where the GDPR does not require an organization to conduct a DPIA, the process may help the organization:

- Assess risks before processing data.
- Mitigate risks by demonstrating that it took actions to comply with GDPR requirements.

(See Article 29 Working Party, WP 248.)

TRANSFERRING PERSONAL DATA

In addition to needing a lawful basis to process personal data, a party must have a lawful basis to transfer data outside of the EU for discovery purposes.

Transfers to the US are particularly problematic because the GDPR permits data controllers to transfer personal data to only those countries that adequately protect personal data (GDPR, Article 45; Recital 103). The European Commission does not consider the US to offer adequate privacy protections, which means that organizations must meet certain GDPR requirements before transferring personal data to the US (GDPR, Article 46).

For purposes of EU-US data transfers for US disputes, the GDPR provisions most likely to be invoked require the transfer to either:

- **Be subject to appropriate safeguards.** Adequate safeguards may include:
  - a legally binding and enforceable instrument between public authorities or bodies (GDPR, Article 46(2)(a));
  - binding corporate rules (GDPR, Article 46(2)(b), Article 47); or
  - standard data protection clauses adopted or approved by the European Commission, such as model contract clauses (GDPR, Article 46(2)(c) and (d)), an approved code of conduct (GDPR, Article 46(2)(e), Article 40), or an approved certification mechanism (GDPR, Article 42).

  These provisions do not permit onward or additional transfers to data processors or data controllers, which includes parties in US litigation.
- **Involve the EU-US Privacy Shield Framework.** The EU-US Privacy Shield Framework, adopted by the European Commission in July 2016 (see Commission Implementing Decision (EU) 2016/1250), provides a means to transfer data from the EU to the US if organizations undergo annual self-certification and verification and commit to a set of privacy principles which, together, are deemed to provide an adequate level of protection of personal data. However, on July 4, 2018, the EU Parliament adopted a resolution calling for the Privacy Shield Framework to be suspended unless US authorities are fully compliant by September 1, 2018.
- **Constitute a one-time transfer to serve compelling, legitimate interests.** A data controller may seek to transfer personal data where the transfer:
  - is not repetitive;
  - concerns a limited number of data subjects;
  - is necessary for purposes of compelling legitimate interests that are not overridden by the data subject's interests or rights and freedoms; and
  - is subject to suitable safeguards to protect the personal data during and after the transfer (however, it remains to be seen whether a party can provide adequate safeguards where the data will be produced in a US dispute).

  The data controller must inform both the data subjects and the supervisory authority of the transfer and the compelling legitimate interests pursued. (GDPR, Article 49(1); Recital 113.)

Where a litigant cannot apply any of these approved bases to transfer data, it may attempt to invoke the GDPR exemption permitting transfers where they are necessary for the establishment, exercise, or defense of legal claims in a non-EU country (GDPR, Article 49(1)(e)). However, where a party seeks to invoke this exemption, the transfer must be "occasional and necessary" for purposes of:

- Judicial proceedings.
- Administrative or out-of-court proceedings.
- Proceedings before regulatory bodies.
- Criminal or administrative investigations.

The nuances and boundaries of the necessity requirement have not yet been clearly defined. Any data that a litigant intends to transfer should be rigorously analyzed to identify the scope of affected data subjects and determine whether the data should be anonymized or pseudonymized.

- Formal pretrial discovery proceedings, including to commence a litigation or to seek approval for a merger.

(GDPR, Recital 111; Article 29 Working Group, WP 262.)

The mere possibility that litigation proceedings may arise in the future, however, is insufficient to justify a data transfer. This can pose challenges where, for example, a party must implement a cross-border litigation hold or perform an early case assessment before litigation arises.

Search Cross-Border Legal Holds: Challenges and Best Practices for information on crafting a cross-border legal hold policy and implementing a US-style legal hold abroad.

Search The Advantages of Early Data Assessment for information on using early data assessment to search, organize, and cull a collection of electronically stored information before it is fully processed.

The nuances and boundaries of the necessity requirement have not yet been clearly defined. Therefore, any data that a litigant intends to transfer based on this provision should still be rigorously analyzed by counsel to identify the scope of affected data subjects and to determine whether the data can and should be anonymized or pseudonymized before any transfer occurs.

Notably, under the GDPR, judgments and decisions from courts, tribunals, or administrative authorities in a "third country" may be enforceable only "if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter" (GDPR, Article 48; Recital 115). This provision might call into question whether US litigation proceedings can ever be considered a lawful basis for the processing and transfer of data where the litigation is not also somehow tied to a mutual legal assistance treaty. However, the "without prejudice to other grounds for transfer" clause appears to leave open the ability to transfer data under other provisions discussed above.

Search Cross-Border Transfers of Personal Data Under the GDPR for information on how the GDPR affects the transfer of personal data between the UK and countries outside the EEA.

RETAINING PERSONAL DATA

The GDPR restrictions on retaining personal data stem from the principle that personal data should be kept in a form that permits data subjects to be identified only for as long as needed to satisfy the purposes behind the processing of the personal data (GDPR, Article 5(e)).

The importance of this principle has been amplified by the "right of erasure," commonly known as the right to be forgotten. The right of erasure permits a data subject to have an organization delete personal data it possesses or controls that concerns the data subject "without undue delay," including removing personal data that the organization made public, if any of the following circumstances exist:

- The personal data is no longer needed to serve the purposes for which it was collected or otherwise processed.
- The data subject withdraws her consent and there is no other legal ground for the processing.
- The data subject formally objects to the processing and there are no overriding legitimate grounds for the processing.
- The personal data was unlawfully processed.
- The personal data must be erased to comply with a legal obligation in the EU or in an EU jurisdiction to which the data controller is subject.

(GDPR, Article 17.)

The right of erasure is a qualified right rather than an absolute right. A data controller's legitimate interests in the personal data may in some circumstances override the interests of the data subject seeking to exercise the right. Additionally, the right of erasure does not apply to processing personal data to establish, exercise, or defend legal claims which, as discussed above, may encompass US disputes. (GDPR, Article 17(3).)

Search Data Subject Rights Under the GDPR for more on the right of erasure.

The Sedona Conference Resources

The Sedona Conference provides various resources to help organizations and their counsel navigate cross-border discovery. Key principles from this guidance include the following:

- Counsel and parties should demonstrate due respect for foreign data protection laws.
- Where full compliance presents a conflict of law, a party's conduct should be judged by a standard of good faith and reasonableness.
- Parties should limit the scope of preservation and discovery to limit conflicts of law.
- Where a conflict with GDPR compliance arises, the parties should enter into a stipulation or obtain a court order.
- Data controllers should be prepared to demonstrate that adequate protections have been implemented to safeguard personal data.
- Data controllers should retain protected data only as long as necessary.

(See The Sedona Conference, International Principles on Discovery, Disclosure & Data Protection in Civil Litigation, available at *thesedonaconference.org*.)

BEST PRACTICES FOR CROSS-BORDER DISCOVERY

Despite the uncertainty that remains, there are some practical steps that can help an organization demonstrate its good faith efforts to maximize GDPR compliance when faced with US discovery demands. For example, counsel should:

- Take full advantage of any US-based discovery to avoid application of the GDPR.
- Analyze potential lawful bases to justify the processing of any personal data.
- Implement appropriate safeguards to protect personal data both before and after a transfer.
- Notify any affected data subjects of the potential processing and transfer and obtain informed and voluntary consent where possible.
- Document all processes and methods counsel have employed in their efforts to comply with the GDPR.

US-BASED DISCOVERY

Perhaps the most obvious means of ensuring GDPR compliance is to conduct as much discovery as possible within US borders. For example, counsel should:

- Assess whether a litigant can comply with US discovery obligations without seeking foreign discovery.
- Object to cross-border discovery requests, particularly where they are disproportional or duplicative.
- Seek judicial intervention as needed, and be prepared to demonstrate the cost and burden of searching for data abroad and complying with the GDPR.
- Ask requesting parties to use existing international mechanisms such as the Hague Evidence Convention and letters rogatory.

LAWFUL BASIS JUSTIFICATION

Identifying a lawful basis under the GDPR to justify processing personal data is perhaps the most labor-intensive but critical step to maximize compliance. To help inform and support this analysis, counsel should:

- Understand the specific rules and protections in each EU jurisdiction where the applicable data resides, including any relevant country-specific rules and practices. Counsel can consult local data privacy counsel about these jurisdictional rules and local best practices, which may involve seeking agreements with works councils in some countries.
- Set out the details of documents that must be reviewed or collected, including email accounts to be searched, persons to being interviewed, relevant time periods, and relevant file types.
- Apply reasonably narrow search parameters to electronically search for only documents that are necessary (rather than merely potentially or tangentially relevant) to resolve contested issues in the dispute.
- Review any search hits within the EU to minimize the scope of a cross-border transfer, or remove any personal information from the data before transferring it to the US for review. However, this may not be a realistic solution in many disputes, depending on the amount of personal information included in the data.
- Immediately delete any collected data as soon as counsel determine that the data is unnecessary.
- Re-review the data at key points in the litigation, such as after the dismissal or settlement of particular claims or the dismissal of certain parties, to identify and delete any data that is no longer needed.
- Consider potential compliance obligations when additional processing is performed on the preserved data.
- Ensure the data controller and any data processors (typically litigation support vendors) sign an appropriate data processing agreement that provides assurances about adequate privacy protection for personal data. Where possible, use a data processor that:
  - is located in the country where the data resides; and
  - has implemented appropriate privacy safeguards.

  (For more information, search Data Processor Obligations Under the GDPR on Practical Law.)

Search Overview of EU General Data Protection Regulation for more on the lawful bases under the GDPR that can justify processing personal data.

Counsel should arrange to delete any collected data as soon as it is no longer needed. Additionally, counsel should ensure that all parties delete any provided data when the dispute is resolved.

DATA COLLECTOR SAFEGUARDS

Counsel should confirm that the data collector has enacted appropriate safeguards to protect collected personal data both before and after a data transfer. Common safeguards include:

- **Security measures.** Data encryption or other reasonable protections should be in place when handling personal data. This is useful for both the data transfer and the subsequent storage and handling of the data in the US.
- **Confidentiality agreements and protective orders.** These agreements and orders can help shield the confidentiality of personal data that is included in the transferred data. (For more information, search Protective Order for Documents Protected by Non-US Data Protection Laws on Practical Law.)
- **Restricted access to transferred data.** Counsel should permit individuals to view the data only on an as-needed basis, and should document any instances where someone has accessed the data.
- **Anonymizing software tools.** Software or service providers that can anonymize or pseudonymize personal data even before review or transfer of the data can help mitigate the risk that personal data will be improperly processed or transferred. Only a small minority of documents produced for discovery in US litigation are used in depositions or at trial. Even anonymized or pseudonymized versions of documents typically contain enough information for trained reviewers to determine their potential importance for resolving disputed issues in the litigation. Where reviewers determine that an anonymized document is highly relevant, an organization might need to produce that document in its original, pre-anonymized form. Yet by anonymizing documents before the initial review, an organization can filter out most (indeed, all but the most relevant) documents from further processing or transfer, thereby minimizing any necessary processing or transfer of key documents with personal data still intact.
- **Inspection instead of production.** Counsel should consider requiring the requesting party to examine the data at a secure location (preferably before the data transfer) where possible rather than producing documents containing personal data. After that inspection, counsel can arrange for the transfer of only truly necessary documents, which generally make up a small portion of the original data universe.
- **Discarding of unneeded data as soon as possible.** Counsel should arrange to delete any collected data as soon as it is no longer needed. Additionally, counsel should ensure, through a case management, confidentiality, or protective order and through agreements with litigation support providers, that all parties must delete any provided data when the dispute is resolved. To confirm compliance with this obligation and ensure the data was deleted on a timely basis, counsel should follow up with the data controller, any litigation support vendors, and opposing counsel (who must then follow up with their clients and litigation support vendors).

NOTIFICATION AND CONSENT

Counsel should notify data subjects when their data is being processed or transferred for a US dispute. This information may also be contained in an organization's privacy policy, but boilerplate notices in a privacy policy generally do not meet notification requirements under the GDPR. Instead, counsel should consider providing specific notices, to the extent practicable, when data is being transferred for a particular dispute.

Moreover, counsel generally should avoid relying on consent as the primary basis for any data processing or transfers. If counsel must seek consent, they should:

- Take steps to ensure and document that the data subject's consent was truly informed, specific, voluntary, and revocable to the extent possible.
- Put measures in place to address the exercise of data subject rights, including any objections to the processing or transfer and requests to access the personal data, as applicable.

RECORDKEEPING

In light of the GDPR's new accountability requirement, counsel should maintain detailed documentation of all procedures used in connection with processing or transferring personal data and constantly monitor the data controller's compliance with data protection laws. In general, all technical and organizational procedures and data subject notifications must be recorded. An organization may use this information when demonstrating its compliance during any audits.

The authors gratefully acknowledge the contributions to this article by their colleagues in the firm's Information Technology, Privacy & Data Security Group in London, Munich, Paris, Houston, and New York.