



2025 International Client Seminar
March 6-9, 2025

“Stuck in the Middle With You”

*Ensuring Compliance with U.S. Discovery Obligations
Without Running Afoul of European Privacy Laws*

Kim Champion
Moderator

CHARLES RUSSELL SPEECHLYS
Paris, France
kim.champion@crsblaw.com

Elisa Lemus García
BUFETE BARRILERO
Madrid, Spain
e.lemus@barrilero.es

Woods Parker
HUIE, FERNAMBUCQ & STEWART, LLP
Birmingham, AL
wparker@huielaw.com

Ensuring Compliance with U.S. Discovery Obligations Without Running Afoul of Foreign Privacy Laws

Nearly a decade after the enactment of the EU’s General Data Protection Regulation (“GDPR”), attorneys, and often, members of the judiciary, continue to lack a basic understanding of the burdens imposed by GDPR and other foreign privacy regulations, including the ways in which GDPR compliance may be implicated by even the most basic discovery requests. This often results in an impossible choice for litigants who maintain foreign design or manufacturing operations—sanctions in U.S. courts for failure to comply with discovery obligations or draconian fines for violation of GDPR. However, there are tools to get ahead of GDPR compliance issues by educating judges and opposing counsel on the issues, as well as an understanding to be gained from analyzing guidance and rulings of U.S. courts and EU advisory bodies evaluating these tensions. Further, while burdensome, compliance with EU discovery in a GDPR-compliant manner is not impossible, especially when issues are identified early.

The GDPR Framework

Enacted in 2018, the GDPR is an extraordinarily complex framework of laws and guidance consisting of 99 articles and a non-binding preamble that itself contains 173 recitals.¹ The GDPR adopted much of the language of its predecessor, the EU Data Protection Directive.² Generally, the GDPR places restrictions on the “Processing” of “Personal Data.”³ The “Processing” of Personal Data is generally defined by the GDPR in an extremely broad manner, encompassing virtually all uses of the documents, including, collection, analysis, or review, and transfer to a third country. “Personal Data” also is defined in an extremely broad manner. It includes any information related to an identified or identifiable natural person concerning the personal or material of an identifiable natural person.⁴ Information such as name, job title, email address, or telephone numbers all qualify as “Personal Data” under GDPR.

No step of processing personal data can occur unless one of six specifically enumerated conditions under the GDPR applies, and each step must comply with fair information processing principles.⁵ Moreover, transfer to a third country may only occur: 1) to a nation with an “adequate” level of protection (not the U.S.); or 2) in compliance with one of the seven explicitly stated exceptions.⁶ This generally means that transfer of documents containing personally identifiable information to the United States (and most other countries) is prohibited, except as authorized. U.S. litigants should be familiar generally with the legal requirements for processing and enumerated exceptions to the transfer prohibitions, as well as the narrowness with which the EU interprets them to easily address assertions of inapplicability by requesting parties.

Penalties for noncompliance with the GDPR are draconian—up to € 20 million or 4% of corporate revenue.⁷

The Tension Between U.S. Discovery Laws and GDPR

The obligation to produce applies to any documents within the “possession, custody or control”⁸ of a responding party. Notably, the geographic location of the documents is irrelevant.

Stuck in the Middle With You

Thus, if a U.S.-based company has access to EU servers, data contained within such servers is generally discoverable. Courts almost universally hold that foreign privacy laws like GDPR do not act as a bar on production pursuant to civil litigation discovery obligations in the U.S.⁸ Indeed, the U.S. Supreme Court, dating back to 1958, has explicitly held that the existence of foreign privacy laws does not render EU records out of the “control” of U.S. litigants.⁹ On the other hand, GDPR is explicit that a U.S. discovery order does not relieve a data controller of its GDPR obligations. Article 48 provides that “[a]ny judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner 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.”

Common Examples of GDPR Implications in Discovery

- Requests for engineering drawings for products designed in the EU (likely to contain the name of EU engineers)
- Requests for communications relating to the design of a product developed in the EU (likely to contain both the names of EU citizens and require collection of documents from EU custodians)
- Requests for “other incident” information involving lawsuits or claims overseas (will contain the Personal Data of claimants)
- Catchall requests for “all documents” relating to an aspect of a product (likely to contain both the names of EU citizens and require collection of documents from EU custodians)

Two Layers of Legality, Each With its Own Exceptions

As referenced above, for each step of data processing to be considered lawful, one of six requirements set forth in Article 6 must apply. Then, for a data processor to transfer the data to the U.S., one of seven exceptions, set forth in Article 49, to the rule against transfer must also apply.¹⁰ The Article 6 conditions and Article 49 exceptions are similar, but not identical, and the EU has interpreted the provisions individually.¹¹

Layer 1: Data Processing

To process personal data, one of six lawful conditions of Article 6 must apply to the processing. The four conditions that arguably might apply to processing data for purposes of litigation are below, along with their limitations:

1. **Consent:** Data processing is permitted if the data subject has explicitly consented to the transfer, having been informed of the possible risks of the transfer.¹²
 - a. **Limitations:**
 - If an employee feels he or she must consent as a term of employment, the consent is invalid.¹³ Some EU states take the position that employees can *never* freely consent.

- Consent may be withdrawn at any time.¹⁴
- 2. **Legal Obligation:** Data processing is permitted when necessary to comply with a legal obligation, to which *the controller* is subject.¹⁵
 - a. **Limitation:** Legal obligation must be EU or member state law (EU entity—not U.S. affiliate—is the controller). An obligation is insufficient.¹⁶
- 3. **Public Interest:** Data processing is permitted necessary for carrying out a task in the public interest.¹⁷
 - a. **Limitation:** In interpreting a similar provision for data transfer (discussed below), the EU Working Party held that the provisions of GDPR’s predecessor law required that the “public interest” must implicate the EU member state—and not merely the judicial system of a third party.¹⁸
- 4. **Catchall: Legitimate Interests of Data Controller:** Data processing is allowed if necessary for “the purposes of 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”¹⁹
 - a. **Limitation:** The legitimate interest (defending or prosecuting U.S. litigation) is likely to be that of the U.S. litigant, and not that of the data controller. Further, the EU view of “fundamental rights” likely will override any interest of U.S. litigant.²⁰

Layer 2: Data Transfer to the United States

To transfer personal data to another country, one (1) of seven (7) exceptions, conditions, or “derogations,” to the GDPR’s prohibition of transfer must apply. The three (3) derogations that arguably might apply to processing for purposes of litigation are below, along with their limitations:

1. **Consent:** Data processing may be permitted if the data subject has explicitly consented to the transfer, having been informed of the possible risks of the transfer.²¹
 - a. **Limitation:** In addition to the data processing consent requirements for consent discussed above, based on Article 49 language, consent cannot be blanketed consent (such as in an employment contract), but must relate to a specific data transfer.²²
2. **Public Interest:** Transfer may be permitted if necessary for important reasons of public interest.²³
 - a. **Limitations:** (see above limitations for the same provision with respect to data processing)
3. **Establishment, exercise, or defense of legal claims:** Transfer permitted if necessary for the “establishment, exercise or defen[s]e of legal claims.”²⁴
 - a. **Limitation:** The independent EU advisory board interpreted this provision of the GDPR’s predecessor law in an extremely narrow manner, meaning only to include cases where the data controller itself (that is the EU affiliate) is a party to the action.²⁵

Thus, the lawful processing conditions and exceptions to the transfer prohibition are by no means a guarantee of GDPR compliance in the context of U.S. discovery obligations.

What is “Processing” Anyway?

As discussed herein, the “Processing” of Personal Data is defined by the GDPR in an extremely broad and all-encompassing manner, meaning to include virtually all uses of the documents, including, their collection, analysis, review, or transfer to a third country. The steps that might be required for the production or use of documents in U.S.-based discovery include:²⁶

- Collection of an individual EU citizen’s documents, whether they contain Personal Data on their face or in metadata;
- Collection of documents from an EU source that contain an individual’s Personal Data on the face of the documents or in metadata;
- Analysis of documents containing Personal Data within the EU;
- Transfer of documents containing Personal Data to the United States; and
- Use of documents containing Personal Data in the United States, whether for analysis or production in U.S. litigation.

So You’ve Been Ordered to Produce EU Personal Data: A Suggested Plan for Compliance . . . And its Burden

You might be asking yourself why this section on compliance with a court order implicating the GDPR would come before the discussions below concerning getting ahead of discovery disputes or steps to combat Motions to Compel. Very simply, an understanding of the burdens of GDPR compliance is crucial to being able to explain to Courts why GDPR-implicating discovery should be disallowed:

Imagine a broad Rule 34 Request for “all communications relating to the consideration of safety features in model year 1998 Widgets” designed and manufactured by your client. You are aware that the 1998 Widget was designed in Germany by a German engineering team and that most responsive documents were maintained by individual members of the German engineering team or on German servers. Collecting responsive documents will certainly implicate GDPR’s processing restrictions and possible transfer to the U.S. will implicate both processing and transfer restrictions. A burdensome, but generally GDPR-compliant mechanism for collection and review is suggested as follows:

1. Identification of EU Custodians: Obviously, the first step in compliance will be the identification of the EU custodians whose documents will be collected. Initial discussions with the custodians should include the nature of the documents, including whether Personal Data is implicated, and the volume of any potential document set.
 - a. A Cautionary Tip for the Earliest Stages of EU Data Collection: Often, EU

employees, seeking to be helpful to U.S. attorneys, may attach documents containing Personal Data in emails to U.S. attorneys. For example, an EU custodian may respond to an initial query from in-house counsel in the U.S. by stating that they are only in possession of a very discrete number of documents, but also attaching those documents to the email. This is an inadvertent violation of GDPR. When reaching out for the first time to EU custodians, consider beginning emails with the following note: “CAUTION: IN RESPONDING TO THIS EMAIL, PLEASE DO NOT ATTACH ANY DOCUMENTS WITHOUT PRIOR DISCUSSION WITH [COUNSEL].”

2. Consent of EU Custodians to Collect: Upon determining the appropriate custodians for collection, written consent must be obtained before any further processing can occur. Remember that consent must be freely given and cannot be acquiesced to by boiler plate employment or other contractual language.
3. Collection/Redaction in EU:
 - a. If the volume of documents is low, the best course of compliance for GDPR is for the individual custodian to redact the PII in the documents because review and redaction of the documents would not constitute “processing” under GDPR. Thorough discussions with the custodian must occur such that the custodian understands the required redactions and how to scrub metadata.
 - b. For higher volume document collections, review by attorneys or data privacy officers only for purposes of PII redaction, may be required. Such review without analysis arguably is not “processing.” However, simultaneous review for relevance or responsiveness would constitute data processing and be impermissible.
 - c. This may include a line-by-line review of documents, since the names or emails or other Personal Data implicated may be unknown before review of the documents.
 - d. If redaction is impossible, the individual consent of each identifiable individual’s PII must be obtained before transfer can occur to the U.S.
4. Transfer: Once Personal Data has been removed, the transfer to the U.S. is permissible.
5. Review for Responsiveness/Relevance: Not until all Personal Data has been removed in the EU can the documents be reviewed for responsiveness and relevance.
6. Production: Prior to production, care must be taken to again ensure no metadata containing Personal Data remains or has been introduced during transfer.

Getting Out Ahead of GDPR-Implicating Disputes

There are a handful of ways to proactively educate courts and judges on the burdens of GDPR compliance. However, they all require early identification of potential issues. Therefore, knowledge of a product’s design history is crucial. A few tools are available in United States Courts.

- **Rule 26 Conferences and Reports**: A discussion of the implications of GDPR due to a product’s design history are appropriate during Federal Rule 26 Conferences as they relate to discovery. Corporate defendants may seek agreements that discovery will be limited to U.S. sources and individuals with knowledge in the United States. In the likely event the parties disagree, the corporate defendant can still assert their position in the

Stuck in the Middle With You

Report to the Court. While not binding, this represents a showing of good faith, which may be a factor in favor of disallowing the discovery, as discussed further herein.²⁷

- **Informal Discovery Conferences:** Upon service of discovery implicating Personal Data, requests for an Informal Discovery Conference (“IDC”), or similar mechanism, where available, may provide a corporate defendant with an opportunity to educate judges on the burdens of GDPR compliance and penalties for noncompliance.
- **Protective Orders:** Motions for a protective order based on burdens of compliance in the context of Rule 26’s proportionality requirement (discussed below) may force judges to review a corporate defendant’s arguments and make findings that limit the scope of foreign. Once confronted with the GDPR’s burden and objection obligations, courts may limit EU discovery when confronted with the possibility of moving trial dates or extending scheduling orders due to extensive time periods require consent, data processing, and redaction. Declarations by outside counsel (preferably EU counsel) outlining burdens of compliance are helpful.

Legal Arguments Against Burdensome EU Discovery

Once a Motion to Compel has been filed, and a U.S. litigant is tasked with arguing to a Court that the GDPR-implicating discovery should be disallowed, the U.S. litigant should argue two (overlapping) theories for why it should not be required to comply: 1) Rule 26’s Proportionality Requirement; and 2) The factors, endorsed by the U.S. Supreme Court, set forth in the Restatement (Third) on Foreign Relations Law.

Proportionality

As U.S. litigants know, in 2015, the Federal Rules of Civil Procedure were amended to include a requirement that discovery must be “proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties’ relative access to the information, the parties’ resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.”²⁸ As highlighted above, the burdens of compliance with GDPR are often extreme. Judges, unfamiliar with these burdens, may be persuaded that the burdens of such discovery outweigh its benefit, particularly as to overbroad document requests, and when Motions or Responses to Motions are supported by Declarations from EU counsel outlining compliance.

U.S. Courts’ Approaches To the Tension of U.S. Discovery Law and GDPR

Generally, United States courts follow the Restatement (Third) on Foreign Relations Law, and the direction which sets forth five factors for courts to evaluate when deciding whether to order production that may conflict with a party’s foreign privacy law obligations, with the burden on the party opposing disclosure.²⁹ Those factors are:

The Restatement Factors

Stuck in the Middle With You

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 United States;
4. The availability of alternative means of securing the information;
 - i. Some courts find this factor determinative. If easily obtained elsewhere, “there is little or no reason to require a party to violate foreign law.”³⁰
 - ii. Alternative must be “substantially equivalent.”³¹
5. The extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the country where the information is located.
 - i. Courts often cite this as the most important factor, and, unsurprisingly, favor the U.S. judicial interest in disclosure of the EU documents.³²
 - ii. Courts often find that a protective order is sufficient to diminish the foreign interest.³³

These factors, “relevant to any comity analysis,” were also endorsed by the United States Supreme Court in 1987 in the context of a request for EU documents in the *Societe Nationale Industrielle Aerospatiale* case.³⁴

Additional Factors

Some courts consider additional factors, such as:

- The hardship of compliance on the party or witness from whom discovery is sought (Second Circuit;³⁵ Ohio³⁶) or the hardship that inconsistent enforcement would impose upon the person (Ninth Circuit³⁷);
- the good faith of the party resisting discovery (Second Circuit³⁸);
- the extent to which enforcement by action of either state could reasonably be expected to achieve compliance with the rule prescribed by that state (Ninth Circuit;³⁹ Ohio⁴⁰).

Conclusion

U.S. litigants rightfully should be intimidated by the prospects of potential GDPR compliance in a discovery order. However, familiarity with the GDPR regulatory scheme and its burdens provide opportunities to educate courts and opposing counsel of compliance issues and allow litigants to develop early plans for compliance strategies.

¹ Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR]; see also, General Data Protection Regulation “GDPR,” Intersoft Consulting, <https://gdpr-info.eu> (last visited February 4, 2025).

² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, p. 31 (23 Nov. 1995).

³ See generally *id.* art. 6; art. 49.

⁴ See *id.* art. 4(1). “Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[.]”

⁵ See *id.* art. 6; see also William McGeeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 966 (2016); see also Gabriela Zanfir-Fortuna & Teresa Troester-Falk, *Future of Priv. F. and NYMITY, Processing Personal Data on the Basis of Legitimate Interests under the GDPR: Practical Cases 3* (2018) (citing GDPR art. 5(1)(a)).

⁶ See GDPR art. 49.

⁷ GDPR art. 83 (5).

⁸ See FED. R. CIV. P. 34(a).

⁸ See, e.g., *Societe Internationale v. Rogers*, 357 U.S. 197, 205 (1958) (hereinafter *Societe Internationale*) ; *Finjan, Inc. v. Zscaler, Inc.*, No. 17-cv-06946-JST (KAW), 2019 U.S. Dist. LEXIS 24570, at *4–5, *10–11 (N.D. Cal. Feb. 14, 2019); *Arigna Tech. Ltd. v. Nissan Motor Co., Ltd.*, No. 2:22-cv-00126-JRG-RSP, 2022 U.S. Dist. LEXIS 135245, at *5, *9 (E.D. Tex. July 29, 2022).

⁹ *Societe Internationale*, 357 U.S. 197, 205 (1958).

¹⁰ GDPR art. 6; art. 49.

¹¹ This document sometimes cites to issuances of the “Article 29 Working Party Guidelines.” The Working Party was a group of EU data protection authorities that issued guidance as to the provisions of GDPR’s predecessor, the Data Protection Directive. Several provisions of the DPD are similar or identical to GDPR’s provisions, and the Working Party Guidelines with respect to those provisions are authoritative.

¹² GDPR art. 6(1)(1). The requirements for Consent are set forth in GDPR art. (7).

¹³ GDPR art. 7(4).

¹⁴ GDPR art. 7(3).

¹⁵ GDPR Art. 6(3).

¹⁶ See Art. 29 Data Prot. Working Party, WP 117, Opin. 1/2006 on the Application of EU Data Protection Rules to Internal Whistleblowing Schemes in the Fields of Accounting, Internal Accounting Controls, Auditing Matters, Fights Against Bribery, Banking and Fin’l Crime, 00195/06EN (1 Feb. 2006).

¹⁷ GDPR art. 6(5).

¹⁸ Article 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, 2095/03 EN, WP 114, (November 25, 2005), p. 15, para. 2; see also Article 29 Working Party discussed the same issue with regard to Article 49 GDPR in its Working Paper 261, Guidelines on Article 49 of Regulation 2016/679 (Updated), Adopted on 6 February 2018. It states (page 11): “only public interests recognized in Union law or in the law of the Member State to which the controller is subject can lead to the application of this derogation.”

¹⁹ GDPR art. 6(6).

²⁰ See 5 COMPUTER LAW: A Guide to Cyberlaw and Data Privacy § 52.12[3].

²¹ GDPR art. 49(1)(a); art. (7).

²² GDPR art. 49 (1)(a).

²³ GDPR art. 49(1)(d).

²⁴ GDPR art. 49(1)(e).

²⁵ See Report of the Berlin Commissioner for Data Protection and Informational Freedom, Section 11.3 on the Working

Group “International Data Traffic,” (December 31, 2009); Working Paper 261 on Article 49(1)(e) GDPR, Article 4(2).

²⁶ See GDPR, *supra* note 2, at art. 4(2). “Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

²⁷ See, e.g., *Minpeco S.A. v. Conticommodity Servs., Inc.*, 116 F.R.D. 517, 523 (S.D.N.Y.1987); *Reino De Espana v. Am. Bureau of Shipping*, No. 03 Civ. 3573, 2005 U.S. Dist. LEXIS 15685, at *10–11 (S.D.N.Y. Aug.1, 2005).

²⁸ FED. R. CIV. P. 26(b).

²⁹ See, e.g., *Societe Nationale Industrielle Aerospatiale v. United States Dist. Court for S. Dist.*, 482 U.S. 522, 544 n. 28 (1987) (hereinafter *Aerospatiale*); *Volkswagen, AG v. Valdez*, 909 SW.2d 900, 902 (Tex. 1995) (hereinafter *Valdez*); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES §442(1)(c).

³⁰ *In re Mercedes-Benz Emissions Litig.*, Civil Action No. 16-cv-881 (KM) (ESK), 2020 U.S. Dist. LEXIS 15967, at *17 (D.N.J. Jan. 30, 2020) (hereinafter *Mercedes-Benz*).

³¹ *Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468, 1476 (9th Cir. 1992).

³² See, e.g., *Mercedes-Benz*, 2020 U.S. Dist. LEXIS 15967, at *26.

³³ See, e.g., *Giorgi Global Holdings, Inc. v. Smulski*, CIVIL ACTION NO. 17-4416, 2020 U.S. Dist. LEXIS 89369, at *5–6 (E.D. Pa. May 21, 2020); *Mercedes-Benz*, 2020 U.S. Dist. LEXIS 15967, at *27–28.

³⁴ *Aerospatiale*, 482 U.S. at 544 n. 28.

³⁵ See *Minpeco* 116 F.R.D. at 523 ; *Reino De Espana v. Am. Bureau of Shipping*, No. 03 Civ. 3573, 2005 U.S. Dist. LEXIS 15685, at *11 (S.D.N.Y. Aug. 1, 2005).

³⁶ *Phillips v. Vesuvius USA Corp.*, 2020-Ohio-3285, 21 (Ohio Ct. App. 2020).

³⁷ *Richmark*, 959 F.2d at 1475 (9th Cir.); *United States v. Vetco, Inc.*, 691 F.2d 1281 (9th Cir. 1981).

³⁸ See *Minpeco* 116 F.R.D. at 528 ; *Reino De Espana*, 2005 U.S. Dist. LEXIS 15685, at *11.

³⁹ See *Richmark*, 959 F.2d at 1475; *Vetco*, 691 F.2d at 1288.

⁴⁰ See *Phillips*, 2020-Ohio at 21.