

The Sedona Conference Draft International Litigation Principles, Second Edition (February 2022)



This confidential draft of The Sedona Conference Working Group International Electronic Information Management, Discovery, and Disclosure is not for publication or distribution to anyone who is not a member of Working Group 6 without prior written permission.

The Sedona Conference Draft International Litigation Principles, Second Edition (February 2022)

Drafting Team Members:

Denise E. Backhouse (Drafting Team Leader)

Susan Bennett

Kevin Brady

Oliver Brupbacher

Jerami Kemnitz

David Kessler

Wayne Matus

David Shonka

Lesley Weaver

Phil Yannella

Natascha Gerlach (Steering Committee Liaison)

Taylor Hoffman (Steering Committee Liaison)

The Sedona Conference International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Second Edition) (ILP 2.0)

1. With regard to data that is subject to preservation, disclosure, or discovery in a U.S.-legal proceeding, courts and parties should demonstrate due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws.
2. Where full compliance with both Data Protection Laws and preservation, disclosure, and discovery obligations presents a conflict, a party's conduct should be judged by a court or data protection authority under a standard of good faith and reasonableness.
3. Preservation, disclosure, and discovery of Protected Data should be limited in scope to that which is relevant and necessary to support any party's claim or defense in order to minimize conflicts of law and impact on the Data Subject.
4. Where a conflict exists between Data Protection Laws and preservation, disclosure, or discovery obligations, a stipulation or court order should be employed to protect Protected Data and minimize the conflict.
5. A Data Controller subject to preservation, disclosure, or discovery obligations should be prepared to demonstrate that data protection obligations have been addressed and that appropriate data protection safeguards have been instituted.
6. Data Controllers should retain Protected Data only as long as necessary to satisfy legal or business needs While a legal action is pending or remains reasonably anticipated, Data Controllers should preserve relevant information, including relevant Protected Data, with appropriate data safeguards.
7. Parties and courts should work together to establish reasonable and appropriate data security safeguards for receiving parties to protect against the unauthorized or improper access or disclosure of Protected Data.

I. DEFINITIONS

The following definitions apply to the Principles, commentary, and associated guidance:¹

1. “Data Controller” is the natural or legal person, public authority, agency, or ~~any~~ other body which, alone or jointly with others, determines the purposes and means ~~for~~ of the processing and transfer of Protected Data.²
2. “Data Protection Laws” include any law or regulation, including U.S. laws and regulations, that restricts the ~~usage~~, transfer or disclosure of data, requires safeguarding data, or imposes obligations in the event of compromises to the security or confidentiality of data. The *International Litigation Principles* is intended to apply broadly wherever Data Protection Laws, regardless of national origin, conflict with ~~U.S.~~ common law preservation and discovery obligations, whether those laws take the form of privacy regulations, blocking statutes, or trade secret~~y~~, or other protections.
3. “Data Subject” is any person or entity whose Protected Data is or may be processed, transferred, or disclosed.
4. “Processing” includes any operation, activity, use, or application performed upon Protected Data by automatic or other means, such as collection, recording, storage, alteration, retrieval, disclosure, or transfer.
5. “Protected Data” is any data irrespective of its form (e.g., paper, ESI, images, etc.) that is subject to Data Protection Laws.³
6. “Legal Proceedings” include civil proceedings requiring the discovery of relevant information. The term “Legal Proceedings” does not include—and these International Litigation Principles are not intended to apply in—criminal proceedings or any other government investigations.⁴

¹ Many of the definitions used in the *ILP 2.0* parallel the terms used in the GDPR. We use these definitions intentionally in order to achieve and maintain a common platform of understanding. It should be noted, however, that the *ILP 2.0* is agnostic relative to the national origin of any Data Protection Law and our usage of similar terminology should not be construed as recognition or acceptance of any particular interpretation given to those terms by others, either now or in the future.

² Under the GDPR, a Data Processor who is not also a Data Controller may nevertheless also become subject to a similar level of accountability as a Data Controller or subject to potential joint liability for processing performed on behalf of a Data Controller. GDPR, ~~supra note 2~~ at arts. 28(10) and 82–83.

³ The use of the word “data” in the *ILP 2.0* is intended to convey that the Principles, commentary, and associated guidance apply to all data, from its lowest level of abstraction to any assembly into information and its recordation on any media.

⁴ For specific guidance concerning internal and civil investigations implicating cross-border data transfers, *see* The Sedona Conference, *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices* (“*International Investigations Principles*”), THE SEDONA CONFERENCE (2018) at https://thesedonaconference.org/publication/International_Investigations_Principles.

II. THE SEDONA CONFERENCE INTERNATIONAL PRINCIPLES ON DISCOVERY, DISCLOSURE & DATA PROTECTION IN CIVIL LITIGATION

[Principles 1-3 and comment]

Principle 4

Where a conflict exists between Data Protection Laws and preservation, disclosure, or discovery obligations, a stipulation or ~~court~~ Protective Order should be employed to protect Protected Data and minimize the conflict.

Comment

When a conflict exists between a requesting party's ~~U.S. Litigation~~ Legal Proceedings rights regarding to obtain discovery of relevant data and a responding party's Protected Data obligations, the parties may act creatively and work cooperatively to enter into stipulations or agreements that create private legal obligations. ~~Parties Responding Parties~~ with data disclosure and data privacy conflicts are encouraged to ~~draft~~ engage the requesting party in discussions and enter into stipulations (in the form of a stipulated court order, when possible) that acknowledge ~~and identify the~~ responding party's obligations and conflicting burdens and ~~assign set forth the~~ duties and responsibilities ~~to of~~ the requesting party to ~~protect and dispose~~ ensure of that Protected Data is secure during transfer and retention. In addition, the stipulation should set forth the obligations of the requesting party to return or dispose of Protected Data once the matter is concluded, in a manner consistent with the applicable Data Protection Laws. If the parties cannot cooperatively reach stipulations regarding data protection, then the responding party should seek a protective order. A protective order is commonly used to protect privacy in discovery.⁵

The three-stage approach advanced by the *International Litigation Principles* suggests conflict resolution through stipulations and protective orders. The approach envisions efforts by parties to avoid and minimize potential conflicts of law, including seeking an order from the U.S. court that protects and limits the use of sensitive information such as trade secrets and data covered by Data Protection Laws; a separate order that schedules or phases discovery; and a protocol or legitimization plan that maximizes simultaneous compliance with the Data Protection Law and the preservation, disclosure, and discovery obligations. Depending on the circumstances of the case, some or all of these steps should be applied, recognizing that a stipulation between the parties may be appropriate in circumstances where a court order is not necessary or the matter is not yet before a court.

A. Protective Order or Stipulation

⁵ Seattle Times Co. v. Rhinehart, 467 U.S. 20, 35–36 (1984) (“The prevention of the abuse that can attend the coerced production of information under a State’s discovery rule is sufficient justification for the authorization of protective orders.”); see also King v. Olympic Pipeline Co., 16 P.3d 45, 62 (Wash. Ct. App. 2000) (noting the “need for protective orders to preserve privacy interests” and a court’s “substantial latitude to decide when a protective order is appropriate and what degree of protection is required given the unique character of the discovery process.”).

The ~~A~~ protective order or stipulation should, where possible, be negotiated between the parties and agreed upon, but it may be submitted to the court unilaterally if agreement is not reached. ~~A~~The protective order or stipulation must demonstrate on its face signifies to the appropriate data protection authorities that it is the intent of the parties to respect the Data Protection Laws while complying with the parties' preservation, disclosure or discovery obligations to the U.S. Court are respected and that Protected Data will be treated appropriately by the parties under the auspices and protections of the ~~U.S.~~ court.⁶ The ~~Model U.S. Federal Court~~ Protective Order Guidelines, set forth in Appendix C, ~~contains outline several~~ provisions that extend protections to Protected Data ~~in a format~~ that can be ~~easily~~ tailored to a specific matter as negotiated between the parties or unilaterally ordered by the court.

B. Scheduling Stipulation or Order

Through the use of a scheduling stipulation or order the parties may agree on, or the court may order, deadlines and sequencing for completion of discovery. The primary purpose of the scheduling order is to ensure sufficient time to “legitimize” the processing and transfer of Protected Data. Scheduling contemplates that information that is not subject to Data Protection Laws would be identified, collected, processed, and produced first, thereby minimizing the likelihood that the same or similar information will be required from sources subject to Data Protection Laws.

C. Legitimization Plan

In this third prong, the party responding to discovery would develop a plan setting forth the methodology by which it contemplates preserving, processing, transferring, and producing Protected Data. The legitimization plan should be tailored to each applicable Data Protection Law and should seek to comply with those requirements, as well as with U.S. preservation and discovery obligations. The legitimization plan may be prepared unilaterally or in conjunction with the requesting party and/or data protection authorities. The plan can help to demonstrate compliance with applicable laws and to identify and thereafter resolve processing and transfer concerns before they materialize. The legitimization plan is also useful to prepare *The Sedona Conference Cross-Border Data Safeguarding Process + Transfer Protocol*, set forth in Appendix D and described in the Comment to Principle 5.

⁶ ~~While In the U.S., while~~ protective orders entered by a state or federal court will be accorded due respect by other U.S. courts in civil litigation, documents transmitted to the U.S. under a protective order may still be subject to disclosure to a grand jury in a criminal matter. However, grand jury proceedings are sealed to prevent public disclosure. FED. R. CRIM. P. 6(e)(6). Federal Circuit Courts of Appeals are split in their treatment of grand jury subpoenas for documents subject to a protective order. Three circuits—the 4th, 9th, and 11th— apply a *per se* rule, holding that once documents are within the jurisdiction of the grand jury, they are subject to subpoena, regardless of the existence of a protective order. *See, e.g., In re Grand Jury Subpoena*, 646 F.3d 159 (4th Cir. 2011). Two circuits—the 1st and 3d—apply a balancing test in which there is a strong presumption in favor of enforcing the grand jury subpoena, which may yield to a civil protective order under exceptional circumstances. *See, e.g., In re Grand Jury*, 286 F.3d 153, 162 (3d Cir. 2002). The 2d Circuit gives due deference to the civil protective order and will only allow the grand jury subpoena to proceed upon a showing that the civil protective order was improvidently granted or upon demonstration of “compelling need” or “extraordinary circumstances.” *Palmieri v. State of New York*, 779 F.2d 861, 866 (2d Cir. 1985).

Principle 5

A Data Controller subject to preservation, disclosure, or discovery obligations should be prepared to ~~demonstrate~~ ensure that data protection obligations have been addressed and that appropriate data protection safeguards have been ~~instituted~~ implemented.

Comment

Data Controllers often find themselves subject to Data Protection Laws that may conflict with broad preservation, discovery, or disclosure obligations in U.S. Litigation Legal Proceedings conducted in a foreign jurisdiction. Under such circumstances, the Data Controller may find it beneficial to prepare the documentation following *The Sedona Conference Cross-Border Data Safeguarding Process + Transfer Protocol* (the “Protocol”) set forth in Appendix D, and to integrate the respective processes into its standard processes (“discovery and privacy by design”). The *Protocol* recommends the steps that a Data Controller should undertake to comply with the relevant Data Protection Law as well as U.S.-preservation, discovery, and disclosure obligations. The relevant Data Protection Laws may include an accountability principle or provisions, requiring a Data Controller to be able to demonstrate actual compliance with the law (i.e., not just “compliance on paper”).⁷

The Sedona Conference believes that following the Protocol and including the appropriate persons in the execution and documentation of the *Protocol* will help demonstrate good faith, cooperation, reasonableness, ~~and~~ proportionality, efficiency or any other discovery principles applicable.⁸ ~~Documentation~~ A written record of the steps taken under the *Protocol* may accompany the Protected Data (like a modern day bill of lading that accompanies physical cargo) from one jurisdiction to another. Apart

⁷ See, e.g., GDPR art. 5(2) (“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).” See also, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (ECJ Case C-311/18), (July 16, 2020) (“Schrems II”) and subsequent related guidance [*discussed supra*].

⁸ In Australia discovery is required to be conducted within the overarching purpose of civil proceedings, which is to facilitate the just resolution of disputes according to law as quickly, inexpensively and efficiently as possible. This requires that the cost of resolution is proportionate to the importance and complexity of the matters in dispute - s37M of the Federal Court of Australia Act 1976 (Cth). Practice Note CPN-1: National Court Framework and Case Management (at 10.7) provides that “[a] Request must be proportionate to the nature, size and complexity of the case – i.e. the Request should not amount to an unreasonable economic or administrative burden on the Discovery Respondent.” In Hong Kong it is a requirement in matters involving more than HK\$8 million and at least 10,000 documents that discovery be reasonable, proportionate and economical (Practice Direction – SL1.2). In Singapore, Supreme Court Practice Directions (at PD 48) sets out a framework for proportionate and economical discovery. The matters to be taken into account in assessing proportionality and economics include the number of electronic documents involved, the complexity of the issues, the value of the claim and the ease and expense of ESI retrieval. In the U.K. the overriding objective of the Rules of Civil Procedure (CPR) is to enable the court to deal with cases justly and at proportionate cost (Rule 1.1). This requires dealing with the cases in ways which are proportionate as to the amount of money involved, the complexity of the issues and ensuring that it is dealt with expeditiously and fairly. Part 31 of the CPR sets out the disclosure and inspection of documents, which requires (at 31.5) that the parties must seek to agree a proposal in relation to disclosure that meets the overriding objective prior to the first case management conference.

from compliance with applicable laws, such a record may also help in case the data were to be re-used in other proceedings and contexts.

The documentation may provide some or all of the following information:

1. The purpose for which the Protected Data is being collected and transferred (this would include a brief description of the litigation, investigation, or matter in the United States Legal Proceedings jurisdiction as well as the identification of the intended recipients of the Protected Data)
2. The identification ~~and significance~~ of the Data Protection Laws at issue (the specific sources of Protected Data and their location should be identified, including the locations from which and to where the Protected Data will be transferred), as well as an assessment of the level of protection afforded in the context of the data transfer, in particular as regards to any access by the public authorities of the third country to the personal data transferred, and the relevant aspects of the legal system of that third country
3. An identification of reasonable measures taken to narrow and cull the processing and transfer of Protected Data to only that which is relevant and necessary for U.S.the preservation and discovery purposes (e.g., the use of preliminary questionnaires and interviews, the use of tools and processes to conduct iterative search and retrieval, and de-duplication)
4. The identification of categories of Protected Data collected (e.g., information identifies or is likely to identify the Data Subject, sensitive personal data, trade secret data, any other restricted data)
5. Confirmation that the Protected Data is subject to a protective order or stipulation that may, for example, restrict its use and dissemination, impose confidentiality, compel security measures, provide for Data Subject access, and restrict onward transfer; attaching a copy of the protective order or stipulation
6. Description of the processes and transfers concerning Protected Data to demonstrate transparency (this may include the steps taken—if and as appropriate or feasible—to make information available to or to notify Data Subjects of processing, transfer, and onward transfer of Protected Data (e.g., posting notice, ~~internal circular requesting request for~~ consent))
7. Description of the steps taken to make the remaining Protected Data secure prior to onward transfer (e.g., third-party agreements, nature and type of encryption, access limitation, password protection)
8. Compliance with obligations (if any) to notify others with oversight of data protection (e.g., company's data protection officer, data protection authority, works council)
9. Basis upon which Protected Data is transferred to the U.S.other jurisdiction in accordance with applicable Data Protection Laws (~~such as the legal claims derogation under the 1995~~

~~EU Data Protection Directive⁹), coupled with a protective order for the onward transfer imposing like obligations on the requesting party or otherwise as required by the jurisdiction~~

10. Disposition of processed and transferred Protected Data when no longer needed to fulfill ~~U.S.~~ obligations of the given matter ~~at hand~~ (e.g., destruction or return of Protected Data)
11. Identification and signature of the person or persons ultimately responsible for processing and transferring Protected Data and affixing signatures signifying the steps recorded have been taken

Use of the *Protocol* addresses data protection concerns by providing proof that reasonable processes have been adopted and followed by the parties to provide adequate safeguards to Protected Data processed or transferred for purposes of ~~U.S. Litigation~~ Legal Proceedings, while also recognizing the broad discovery and disclosure obligations many global companies face when subject to ~~foreign~~ government investigations or litigation ~~including~~ in the United States.

⁹—EU Data Protection Directive, *supra* note 1, at § IV, art. 26(d) (“the transfer is necessary or legally required . . . for the establishment, exercise or defence of legal claims”).

Principle 6

Data Controllers should retain Protected Data only as long as necessary to satisfy legal or business needs. While a legal action is pending or remains reasonably anticipated, Data Controllers should preserve relevant information, including relevant Protected Data, with appropriate data safeguards.

Comment

The purpose of Principle 6 is to provide guidance to Data Controllers regarding records retention generally, as well as the specific scope and duration of their obligation to preserve Protected Data that is relevant to [U.S. Litigation Legal Proceedings](#).

The goal of this Principle is to reinforce the ~~records management~~[information governance](#) axiom that records and information do not need to be ~~preserved~~[retained](#) when they are no longer needed for business or legal reasons. This Principle also recognizes that the potential conflict between discovery obligations and Data Protection Laws is lessened by reducing the amount of data that organizations create and retain before preservation and discovery obligations attach.

Many organizations worldwide have become electronic data hoarders. [It is](#) relatively inexpensive to expand storage capacity rather than to apply records management lifecycle discipline to ESI. There are numerous direct and indirect costs and risks, including security risks, associated with unbridled accumulation and retention of data. Legal risks may also arise, especially in the context of data protected by Data Protection Laws, in the over-retention of information.

Organizations should take good faith, reasonable efforts to retain, manage, and dispose of inactive data both on a prospective and retrospective basis. Organizations need not keep all information forever.¹⁰ Rather, reasonable and systematic records management rules can be applied, provided they are applied uniformly, and not in a fashion to avoid a litigant's common law duty to preserve relevant information once the litigant is on notice of actual or reasonably anticipated litigation. Organizations are encouraged to implement data privacy and data protection technologies to further this goal and to design information systems and processes with data protection in mind, e.g., privacy by design.¹¹

Privacy by design is part of the “data minimization” principle (GDPR art. 5(1)(c)), a core principle of the EU Data Protection Laws, whereby data processing should be “adequate, relevant and limited

¹⁰ [In the U.S., this is consistent with the opinion of the U.S. Supreme Court in *Arthur Andersen LLP v. United States*, 544 U.S. 696, 704 \(2005\) \(“Document retention policies, which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business. It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.”\) \(citation omitted\).](#)

¹¹ “The [GDPR incorporates](#) privacy-by-design ~~principle is now codified~~[requirements](#) in Article 25(1):

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical

to what is necessary in relation to the purposes for which they are processed.” The less personal data collected or retained by an organization, the lower the costs and risks to data protection.¹²

This Principle reinforces the notion that the obligation to preserve Protected Data for the purposes of litigation is accompanied by a corresponding obligation to take reasonable steps to protect the reliability, integrity, access, confidentiality, and security of the data while it is being preserved. This includes meaningful efforts to implement privacy-by-design protections in new ESI systems, consistent with the GDPR’s requirements. Data Controllers should continue to observe substantive data protection and confidentiality requirements under Data Protection Laws, such as those in the GDPR, including when they are distributing notice of and requiring compliance with a legal hold notice relating to relevant Protected Data.

This Principle also makes clear that the preservation obligation is limited in duration to the time that a legal action is pending or remains reasonably anticipated. A Commentary from TSC Working Group 1 explains that “reasonable anticipation of litigation arises when an organization is on notice of a credible probability that it will become involved in litigation, seriously contemplates initiating litigation, or when it takes specific actions to commence litigation.”¹³ This limitation should provide assurance to non-U.S. data protection and privacy officials that the duty to preserve is not based upon mere conjecture, supposition, or possibility that legal action may occur at some time in the future.¹⁴

and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

See also, EDPB Guidelines 4/2019 on GDPR Art. 25: Data Protection by Design and by Default (Version 2.0, Adopted on 20 Oct. 2020), available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf.

¹² This area has become a focus of certain GDPR enforcement activity including matters involving over-retention and over-collection of personal information. For example, although subsequently overturned, the Berlin Data Protection Authority (*Berliner Beauftragte für Datenschutz und Informationsfreiheit*) imposed a €14.5 fine against Deutsche Wohnen SE in 2019; the Italian Data Protection Authority (*Garante per la Protezione dei Dati Personali*) imposed a € 16.7 fine against Wind Tre S.p.A in 2020. See generally GDPR Enforcement tracker available at <https://www.enforcementtracker.com/>.

¹³ The Sedona Conference, *Commentary On Legal Holds, Second Ed.: The Trigger & The Process*, 20 SEDONA CONF. J. 341 (2019), Guideline 1 at 366, [https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Legal%20Holds%20\(2\).pdf](https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Legal%20Holds%20(2).pdf).

¹⁴ Unfortunately, there is no black-and-white definition of when litigation is deemed to be “reasonably anticipated.” Like many legal standards throughout the world, it depends upon the facts and circumstances of the particular situation. More frequently than not, preservation conduct is judged long after the fact. As a result, additional guidance on this issue will be welcomed by both U.S. and non-U.S.-based litigants.

Principle 7

Parties and courts should work together to establish reasonable and appropriate data security safeguards for receiving parties to protect against the unauthorized or improper access or disclosure of Protected Data.

Comment (a)

The exchange of evidence among parties is key in common law jurisdictions. Many common law jurisdictions have civil procedure rules similar to U.S. Fed. R. Civ. P. 1, which provides that parties and courts should work toward the “just, speedy, and inexpensive” determination of cases.¹⁵ Restrictions and prohibitions on the transfer and production of materials sought in discovery can result in expensive and time-consuming discovery battles, impeding both aim of speedy and inexpensive resolution of cases. This frustrates the needs of both the producing and receiving parties, and impairs the just disposition of cases. Concerns about the security and improper disclosure of Protected Data often lie at the heart of the restrictions on its transfer across national borders. It is therefore incumbent on all parties and the courts to work together to find practical, legal, and even innovative means of addressing these concerns.

Comment (b)

The Sedona Conference has long recognized that law firms and other legal service providers can be “high value” targets for intrusion, ransomware attacks, and outright theft of personal, sensitive, confidential or privileged information.¹⁶ Reports in the news media provide ample support for these findings.¹⁷ Accordingly, the very ability to transfer protected information across national borders without incurring penalties or other sanctions often depends on the ability of the transferring party to ensure that the transferred data is appropriately secure and protected from unwarranted disclosure.¹⁸ Similarly, any inability of the producing party to provide sufficient assurances concerning the protection of information may delay or impede the ability of requesting parties to obtain information they need for their claims or defenses in Legal Proceedings.

Comment (c)

To overcome concerns about data security and facilitate the production of materials that are both subject to Data Protection Laws and relevant and proportionate to the needs of the case, parties should work together to establish reasonable and appropriate data security safeguards for receiving parties to protect against the unauthorized or improper access to Protected Data. Reasonable and

¹⁵ For example, Australia’s rules state that their “the overriding purpose ... is to facilitate the just, quick and cheap resolution of the real issues in the proceedings” (s 56(1) Civil Procedure Act), while the U.K.’s rules state that their overriding objective is “enabling the court to deal with cases justly and at proportionate cost.” U.K. CPR 1.1.

¹⁶ See WG1 Commentary on data security; and WG11 Commentary on law firm security; FBI briefings/equivalents from other countries].

¹⁷ See, e.g., Paul Weiner and Denise Backhouse, The Case for Requiring Data Security Provisions in Protective Orders, N.Y.L.J., July 29, 2021 (gathering examples of law firms being targeted for attacks).

¹⁸ See, e.g., GDPR Chapter 5 arts 44-49. Nor should counsel overlook their ethical duty to safeguard the confidences of their clients and to protect the confidential information of adversaries and third parties when that information has been entrusted to them.

appropriate data security safeguards are measures that are proportionate to the sensitivity of the information at issue and the harm that may follow from inappropriate disclosures. To be clear, the natural conclusion of the discovery process is that a certain number of discovered documents will ultimately be placed on the court's record, and absent a sealing order, they will be made public. Accordingly, reasonable and appropriate data security safeguards do not, and cannot, mandate the top-level security of discovered materials. They can however include safeguards that limit access to Protected Data to those who need to use or see it, that ensure disclosed Protected Data are reasonably and appropriately protected from theft or other improper handling during the pendency of the Legal Proceeding, and are returned or properly disposed of at the end of Legal Proceeding, except to the extent legal, technical, or ethical obligations mandate their retention by the receiving party.

Comment (d)

In the U.S., Fed. R. Civ. P. 26(c) provides that a trial court “may, for good cause, issue an order to protect a party or a person from annoyance, embarrassment, oppression, or undue burden or expense....”¹⁹ Parties have asked courts to invoke this Rule to impose reasonable and adequate safeguards on receiving parties. At a minimum, such orders further the goals of protecting the producing party from the collateral damage that would result from fines, sanctions, or loss of business reputation in the country hosting the data.

Appendix A: Bibliography & Resources

....

¹⁹ Fed. R. Civ. P. 26(c)(1). See *infra* Protective Order Guidelines at Appendix C.

Appendix B:
Model U.S. Federal Court Order
Addressing Cross-Border ESI Discovery²⁰

UNITED STATES DISTRICT COURT

_____ **DISTRICT OF** _____

_____,)	
)	
Plaintiff.)	Case No.: _____
)	
v.)	Pretrial Order Regarding
)	International Discovery
_____,)	
)	
Defendant.)	
)	

PRETRIAL ORDER RE: INTERNATIONAL DISCOVERY

AND NOW, this day of _____, 20__:

Pursuant to the Court’s authority under Rule 16, Fed. R. Civ. P., the parties having advised the Court [the Court determining from review of the pleadings and any other initial papers in the case] that international discovery may be involved, which may result in substantial delays in concluding discovery, the Court sets special procedures for expediting international discovery.

²⁰ Appendix B is a model Pretrial Order addressing cross-border discovery pursuant to a U.S. Court’s authority under Fed. R. Civ. P. 16. The Hon. Michael M. Baylson (E.D. Pa.), an active member of The Sedona Conference Working Group 6, granted permission to include this *Model U.S. Federal Court Order Addressing Cross-Border ESI Discovery* as an appendix to the *International Litigation Principles*. He developed this model in order to facilitate party discovery outside the U.S. and/or pursuant to the laws of other countries, and to enable courts to promptly rule on any dispute that arises concerning international discovery. This model can be tailored to the specific issues in individual matters. The Sedona Conference WG6 thanks Judge Baylson for his permission to include this model as an appendix. *See* U.S. District Judge Michael Baylson (EDPA), *Model Pretrial Order Re International Discovery*, The 8th Annual Sedona Conference International Programme, Berlin, June 2016.

The provisions of this Order are intended to facilitate the parties taking of discovery outside the United States and/or pursuant to the laws of other countries, and will enable the Court to promptly rule on any disputes that arise concerning international discovery.

It is therefore **ORDERED**:

1. Within _____ days, any party which intends to initiate discovery outside of the United States shall file and serve a statement making disclosure of its intention as of this time, including, but not limited to, the following:

- (a) Whether applications will be made under the Hague Convention or any other treaty.
- (b) Whether Letters Rogatory will be used.
- (c) Whether parties abroad are likely to be deponents in this case.
- (d) Whether documents located outside the United States will be sought for production, including but not limited to, electronically stored information (ESI).
- (e) Whether a party is aware of any blocking statutes or Data Protection Laws that may apply to a request for discovery in a particular country and, if so, identify the country and if possible cite the laws which may be applicable.

2. Within _____ days other parties shall respond to this initial disclosure of foreign discovery, by commenting:

- (a) To what extent it will or will not oppose such discovery.
- (b) If there will be opposition, state concisely the nature of the opposition and the reasons.

3. Within _____ days after the response, the parties shall meet and confer to discuss reaching agreement, or narrowing disputes concerning:

- (a) Conducting discovery outside of the United States, pursuant to the Federal Rules of Civil Procedure or otherwise.

- (b) What date shall be set to complete international discovery.
- (c) Whether any objections will be presented to this Court and, if so, when?
- (d) Whether any protective order will be sought and the extent to which disputes remain as to the contents of a protective order.

4. The Court set a deadline for the initiation of any discovery to take place outside the United States as _____ [date].

5. Motions that may be necessary or appropriate on international discovery issues will be filed no later than _____[date]. Responses will be due within fourteen (14) days, and a reply brief should be filed within fourteen (14) days thereafter.

6. In most countries with blocking statutes and/or data protection rules, an authorized official or judge within that country, may be permitted to negotiate, hear, and/or authorize disclosure of information for use in litigation, even though it is arguable that a blocking statute or data protection law may be construed otherwise. In each party's pretrial disclosures on international discovery, the Court requires each party relying on any such statute or rule to state:

- (a) Its knowledge of this practice as applied to this case;
- (b) Its position on this issue;
- (c) The contact information for the official or judge in each country who is likely to be knowledgeable or authorized to act within that country.

7. The Court anticipates having pretrial conferences with counsel to discuss the course, progress, and any problems in international discovery. The first conference will take place on _____ [date]. Subsequent conferences will be scheduled on a need basis. If problems and issues arise frequently, the Court may schedule conferences on a regular basis.

8. Counsel who do not practice regularly in this District may appear by telephone by notifying Chambers at least 48 hours prior to any pretrial conference.

9. Counsel appearing at these conferences, whether in person or by telephone, shall be authorized to speak on behalf of their client, and shall discuss with their client issues as they are arising so that they can accurately inform the Court of their position.

10. If it appears that certain discovery is relevant in this case, but cannot be secured by normal means of discovery through the Federal Rules of Civil Procedure, or any convention or other recognized international procedure, the Court may itself undertake initiation of communications with any data protection officer of a foreign country or court of a foreign country to determine if such discovery can be authorized, facilitated, and completed on a prompt basis.

11. The obligations stated above apply throughout this litigation, and apply to any initiation of international discovery.

12. The Court encourages the parties to adopt, in this case, the Sedona Conference Principles of International Discovery, Disclosure & Data Protection as follows:

(a) With regard to data that is subject to preservation, disclosure, or discovery, courts and parties should demonstrate due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws.

(b) Where full compliance with both Data Protection Laws and preservation disclosure and discovery obligations presents a conflict, a party's conduct should be judged by a court or data protection authority under a standard of good faith and reasonableness.

(c) Preservation or discovery of Protected Data should be limited in scope to that which is relevant and necessary to support any party's claim or defense in order to minimize conflicts of law and impact on the Data Subject.

(d) Where a conflict exists between Data Protection Laws and preservation, disclosure, or discovery obligations, a stipulation or court order should be employed to protect Protected Data and minimize the conflict.

(e) A Data Controller subject to preservation, disclosure, or discovery obligations should be prepared to demonstrate that data protection obligations have been addressed and that appropriate data protection safeguards have been instituted.

(f) Data Controllers should retain Protected Data only as long as necessary to satisfy legal or business needs. While a legal action is pending or remains reasonably anticipated, Data Controllers should preserve relevant information, including relevant Protected Data, with appropriate data safeguards.

BY THE COURT:

[INSERT JUDGE'S NAME], U.S.D.J.

IN THE UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

_____,)	
)	
Plaintiff.)	Case No.: _____
)	
v.)	Pretrial Order Regarding
)	International Discovery
_____,)	
)	
Defendant.)	
)	

AND NOW, this day of _____, 20____, upon consideration of defendant's Motion for Issuance of Letters of Request Pursuant to the Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters, it is hereby **ORDERED** that said Motion is **GRANTED**.

It is further **ORDERED** that the original executed copies of the Letters of Request attached to defendant's Motion as Exhibits A and B shall be provided to counsel for defendant to serve and execute in conformity with the Hague Convention.

BY THE COURT:

[INSERT JUDGE'S NAME], U.S.D.J.

Appendix C: **Model U.S. Federal Court Protective Order Guidelines**

One element of a layered approach to securing protected data disclosed in litigation in common law jurisdictions is the use of a Protective Order.²¹ Protective Orders provide a vehicle for parties and the court to limit or condition discovery. Parties may stipulate to provisions and submit their agreement to the court requesting that it be entered as an Order, or a party may move to have a Protective Order entered. Violation of a court order carries penalties. Typically, Protective Orders allow producing parties to designate categories of documents and testimony as “Confidential”, then specify limitations on how “Confidential” information may be used. Documents designated

²¹ For example, in the U.S., Federal Rule of Civil 26(c) provides the following for Protective Orders:

(c) PROTECTIVE ORDERS.

(1) In General. A party or any person from whom discovery is sought may move for a protective order in the court where the action is pending—or as an alternative on matters relating to a deposition, in the court for the district where the deposition will be taken. The motion must include a certification that the movant has in good faith conferred or attempted to confer with other affected parties in an effort to resolve the dispute without court action. The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including one or more of the following:

(A) forbidding the disclosure or discovery;

(B) specifying terms, including time and place or the allocation of expenses, for the disclosure or discovery;

(C) prescribing a discovery method other than the one selected by the party seeking discovery;

(D) forbidding inquiry into certain matters, or limiting the scope of disclosure or discovery to certain matters;

(E) designating the persons who may be present while the discovery is conducted;

(F) requiring that a deposition be sealed and opened only on court order;

(G) requiring that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way; and

(H) requiring that the parties simultaneously file specified documents or information in sealed envelopes, to be opened as the court directs.

(2) Ordering Discovery. If a motion for a protective order is wholly or partly denied, the court may, on just terms, order that any party or person provide or permit discovery.

“Confidential” are marked as such when produced. Distribution may be limited to specified people who must as a condition of receipt agree to abide by the Protective Order’s terms and submit themselves to the court’s jurisdiction before receiving Confidential information—a form may be attached as an exhibit to the Protective Order for this purpose. The Order may require the receiving party to maintain the signed forms. Confidential documents are protected during the course of litigation. For example, a Confidential document used as an exhibit to a motion must be filed under seal or redacted.

In the context of cross-border discovery, information subject to data protection laws can be designated as a type of Confidential information.²² Elements of an effective Protective Order for cross-border discovery may include:

- A defined class of protected information, for example:
 - “Confidential under the [specify data protection law]”: this category may include personal information that cannot be redacted.
 - “Highly Confidential under the [specify data protection law] – Attorneys’ Eyes Only”: this designation may include sensitive personal information that cannot be redacted.

²² The following are examples of Protective Orders with cross-border provisions: Restellini v. Wildenstein Plattner Inst., 1:20-cv-04388 (AT) (GWG) (S.D.N.Y. Aug. 9, 2021) (entering stipulated protective order governing disclosure of “private or confidential personal information, including personal data subject to federal, state, and/or foreign Data Protection Laws or other privacy obligations”, including the GDPR); Allianz Glob. Inv’rs GmbH v. Bank of Am. Corp., 18 Civ. 10364 (LGS) (SDA) (S.D.N.Y. Jan. 20, 2021) (sealing documents protected by foreign protection laws, including the GDPR); Bodum Holding AG v. Starbucks Corp., Case 1:19-cv-04280-ER (S.D.N.Y. Dec. 4, 2019) (addressing data subject to the GDPR and the Swiss data protection act), available at https://judicialcaselaw.com/courts/nysd/cases/1_19-cv-04280-ER/127125968439?page=1; In re JUUL Labs, Inc. Marketing Sales Practices, & Prod. Liab. Litig., 19-md-02913-WHO (N.D. Cal., Dec. 13, 2019; In re ZF-TRW Airbag Control Units Prod. Liab. Litig., 19-ml-2905-JAK-FFM (C.D. Cal. Mar. 3, 2020).

- Specified categories of people who may receive Confidential or Highly Confidential information: for example, Confidential Information distribution may be limited to the parties, their agents including their counsel and counsel's staff, experts, eDiscovery services providers, the Court and Court personnel; Highly Confidential – Attorneys' Eyes Only" may be limited to counsel of record and the Court.
- Provisions limiting use to the specific Legal Proceeding: recipients agree to use data only in connection with the specific Legal Proceeding in which it was produced. Include provisions that in the event of a legitimate third-party request or subpoena for the Confidential Information, to the extent permissible by law, the recipient will provide prompt notice to and facilitate objections by the producing party.
- Provisions binding third-party recipients: include as an exhibit a Non-Disclosure Agreement requiring third parties who receive Confidential Information (for example, the parties' experts and eDiscovery services provider) to abide by the terms of the Protective Order, including agreeing to submit to the court's jurisdiction for the purposes of resolving any issues arising under the Protective Order.
- Redaction and pseudonymization: include provisions facilitating the redaction or pseudonymization of protected information, including for example, redacting irrelevant personal information from documents containing relevant information.
- Information security provisions: include provisions requiring recipients of Confidential Information to maintain a written information security program with appropriate technical and organizational measures.
- Cyber incident and breach notification provisions: require recipients of Confidential Information who become aware of data loss or actual or suspected unauthorized

access to provide prompt written notice and to take steps to investigate, remediate and cooperate with the Disclosing Party and if needed, law enforcement investigating the security incident.

- End-of-matter data disposition: specify a protocol for recipients to return or, by written agreement, securely destroy Confidential Information within a set period of time at the matter's conclusion.

Appendix D: The Sedona Conference Cross-Border Data Safeguarding Process + Transfer Protocol

INSTRUCTIONS

The Sedona Conference Cross-Border Data Safeguarding Process + Transfer Protocol (the “*Protocol*”) has two interrelated purposes. First, it is an ease-of-reference guide that identifies common techniques used to achieve best possible legal compliance with conflicting U.S. eDiscovery and discovery rules and extra-U.S. Data Protection Laws when foreign data needs to be processed and transferred for the purposes of U.S. Litigation Legal Proceedings. Second, the *Protocol* creates a record that can be presented to those with regulatory responsibilities for Data Protection, evidencing the steps taken to best comply with Data Protection Laws. The *Protocol* must be customized to record fully the actions undertaken to maximize legal compliance and should include a detailed explanation of the circumstances and factors taken into account. Especially because of the potential for disclosure, the documentation should not itself include Protected Data or privileged information. The following instructions should be used with the chart below:

1. Explain the reasons for preserving or collecting the data. Identify clearly the U.S. Legal Proceedings for which the Protected Data is processed and transferred. If the Protected Data is to be preserved or collected for reasons other than litigation, identify the legal proceeding requiring the processing and transfer.
2. Determine whether data required to be preserved, processed, or disclosed in the U.S. for a Legal Proceeding is subject to Data Protection Laws and, if so, which laws apply. Assess whether alternative, non-protected, sources of that relevant data exist. To the extent possible, produce non-protected sources of data, making production of relevant Protected Data less necessary. Determine the sources of relevant Protected Data, the methods of preservation, if it has been or will be further processed, and where it will ultimately be transferred.
3. Describe measures taken to minimize the processing and transfer of Protected Data, explaining the methodology used to filter and eliminate irrelevant Protected Data. These culling activities may begin with a questionnaire or an in-person interview, followed by iterative use of software tools and other processes, creating a subset of relevant and necessary Protected Data for disclosure. Consider compiling Protected Data locally or in a country that is not subject to the transfer restrictions under the applicable Data Protection law. Identify categories of Protected Data potentially affected by the applicable Data Protection Laws. Consider whether pseudonymization or redaction of protected data is feasible.
4. Describe the various categories of Protected Data that will be processed or transferred by type, including personal and sensitive personal data, trade secrets data, restricted data, consumer data, state secrets, etc.

5. If appropriate, consider ~~using the Model U.S. Federal Court Protective Order (set forth in Appendix C) or similar~~ implementing protective orders, or stipulations with data protection language providing agreed-upon or court-ordered restrictions on the use, disclosure, ~~and~~ dissemination ~~and retention~~ of Protected Data. Consider including options to ~~pseudonymize or redact Protected Data~~ and ~~to~~ designate Protected Data as “Confidential” or “Highly Confidential.” Further, consider restrictions related to the onward transfer of data once it reaches the ~~U.S. third-country destination~~.
6. Strive to provide a transparent processing and transfer protocol to the Data Subjects, identifying impacted Data Subjects and the means to communicate to them the purpose for the processing and transfer of Protected Data, the categories of Protected Data at issue, the duties and obligations attendant to that Protected Data, data protection measures that will or have been put in place, ~~addressing Data Subject rights~~, and such other factors as may be required or appropriate under the circumstances. Such communications to Data Subjects may include postings, one-on-one meetings, group presentations, or notice and acknowledgement documentation ~~requesting consent and providing with~~ question and answer information, in writing or orally, ~~in both English and the~~ ~~and where required including translation to the~~ local language.
7. Identify ~~technical and organizational measures steps taken to used to~~ secure Protected Data by describing the protective measures undertaken by the Data Controller, including, for example, agreements with third parties, use of a protective order, the nature and type of encryption at rest and in transit, limitations on access to the Protected Data, and any other means of securing the Protected Data. Also describe procedures for responding in the event of a data breach ~~or subpoena or other legal request for the data~~.
8. Describe the efforts undertaken if notice is contemplated or required. Others to be consulted may include the Data Controller’s data protection personnel such as data protection officers, data protection authorities with jurisdiction over the Protected Data, or local company organizations such as works councils.
9. Identify mechanism(s) used to legitimize the transfer of Protected Data. For the EU ~~and an increasing number of countries with GDPR-like data protection laws~~, depending on the ~~third-country U.S.~~ recipient and transfer purpose, these mechanisms typically include the use of ~~the Hague Convention and other international treaties~~, Binding Corporate Rules (intra-group transfers only), ~~Model Standard Contractual Clauses~~, ~~Certifications~~, or some other means of satisfying transfer safeguard requirements.
10. Document procedures used to destroy or return Protected Data to the Data Controller when it is no longer necessary.
11. Consider identifying those responsible for overseeing preservation, processing, and transfer of the Protected Data and obtaining their signatures to signify that the steps recorded were in fact taken.

The Sedona Conference Cross-Border Data Safeguarding Process + Transfer Protocol	
ACTION ITEM	INFORMATION
1. Purpose for processing and transfer of Protected Data	Identify the type of legal proceeding for which Protected Data is being processed or transferred (e.g., reasonably anticipated or active civil litigation; government investigation; subpoena) with specific identification information (e.g., case name, docket number, filing location, filing date, description of legal proceeding)
2. Data Protection Laws at issue and specific sources of Protected Data	Identify the each country whose Data Protection Laws are at issue, the specific Data Protection Laws implicated, and the significance of each; identify the location of the Protected Data, where it is processed, and the location to which it will be transferred
3. Measures taken to minimize the processing and transfer of Protected Data	Explain methodology used to narrow and cull Protected Data for processing and transfer purposes to include only relevant and necessary material (e.g., use of preliminary questionnaires and interviews; use of technology and processes to de-duplicate and apply iterative searches; filter and compile information in a country not subject to transfer restrictions under the applicable Data Protection Laws)
4. Categories of Protected Data processed and transferred	Identify categories of Protected Data processed and transferred (e.g., information that is likely to identify the Data Subject, sensitive personal data, trade secret data, restricted data)
5. Limitation on use and dissemination of Protected Data	Identify stipulations or protective orders and their material terms or attach a copy (e.g., Model U.S. Federal Court Protective Order (set forth in Appendix C)); general protective order; confidentiality agreement; Data Protection stipulation)
6. Transparency of processes and transfers concerning Protected Data	Identify steps taken (if and as appropriate or feasible) to make information available or to notify Data Subjects of processing, transfer, and onward transfer of Protected Data (e.g., internal communications; posted notice)
7. Steps taken to secure transferred Protected Data	Identify steps taken <u>to implement technical and organizational measures</u> to secure Protected Data (e.g., third-party agreements, nature and type of encryption, password protection, access limitation and control)

The Sedona Conference Cross-Border Data Safeguarding Process + Transfer Protocol	
ACTION ITEM	INFORMATION
8. Compliance with notification obligations (if any) to others with oversight of data protection	Identify others involved or who may need to be consulted with responsibility for Data Protection implementation (e.g., the company's data protection officer or works council; government data protection authority); explain their involvement and means of notification
9. Bases upon which Protected Data is transferred	Identify Protected Data transfer mechanisms relied on for each U.S. recipient (e.g., EU-Hague Convention or other international treaty , Model Standard Contract Clauses, Binding Corporate Rules, Certifications , or other means of satisfying transfer safeguard requirements); determine whether supplemental analysis is required and identify documentation requirements (e.g., data protection impact analysis, data transfer impact analysis)
10. Disposition of transferred Protected Data when no longer needed	Describe disposition of processed and transferred Protected Data (e.g., destruction or return of Protected Data) when no longer needed to fulfill obligations of the specific matter, and compliance measures in place (e.g., time limit and certification requirements)
11. Person responsible for transfer and processing of Protected Data	Consider identifying the person or persons ultimately responsible for processing and transferring Protected Data and requiring their signed acknowledgement that the steps recorded have been taken