The Sedona Conference Journal

Volume 17 | Number 1 2016

The Sedona Conference Practical In-House Approaches for Cross-Border Discovery & Data Protection

The Sedona Conference

Recommended Citation:

The Sedona Conference, Practical In-House Approaches for Cross-Border Discovery & Data Protection, 17 Sedona Conf. J. 397 (2016).

For this and additional publications see: https://thesedonaconference.org/publications

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual or semi-annual basis, containing selections from the preceding year's conferences and Working Group efforts. The Journal is available on a complimentary basis to courthouses and public law libraries and by annual subscription to others ($95; $45 for conference participants and Working Group members). Send us an email (info@sedonaconference.org) or call (1-602-258-4910) to order or for further information. Check our website for further information about our conferences, Working Groups, and publications: www.thesedonaconference.org.

Comments (strongly encouraged) and requests to reproduce all or portions of this issue should be directed to:
The Sedona Conference, 301 East Bethany Home Road, Suite C-297, Phoenix, AZ 85012 or info@sedonaconference.org or call 1-602-258-4910.

The Sedona Conference Journal® designed by MargoBDesignLLC at www.margobdesign.com or mbraman@sedona.net.

Cite items in this volume to "17 Sedona Conf. J. _____ (2016)."

THE SEDONA CONFERENCE PRACTICAL IN-HOUSE APPROACHES FOR CROSS-BORDER DISCOVERY & DATA PROTECTION*

A Project of The Sedona Conference Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6)

Author: The Sedona Conference

Editor-in-Chief: Jennifer L. Hamilton

Contributing Editors: Taylor M. Hoffman & Jerami Kemnitz

Contributors:

Katelyn Flynn

Cecil A. Lynn III

David Moncure

David C. Shonka

Natasha Williams

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference's Working Group 6. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any organizations to which they may belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Sustaining and Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of

our sponsors, click on the "Sponsors" navigation bar on the homepage of our website.

PREFACE

Welcome to the final, June 2016, version of The Sedona Conference *Practical In-House Approaches for Cross-Border Discovery and Data Protection*, a project of The Sedona Conference Working Group Six on International Electronic Information Management, Discovery, and Disclosure (WG6). WG6 is best known for its groundbreaking publication, The Sedona Conference *International Principles on Discovery, Disclosure and Data Protection* ("International Litigation Principles"). The Sedona Conference *Practical In-House Approaches for Cross-Border Discovery and Data Protection* aims to provide the practical guidance that organizations and In-House counsel need to navigate challenging cross-border data transfer and discovery issues, and to effectively implement the International Litigation Principles.

This publication represents the collective effort of many contributors and members of WG6 who have worked to draft a practical, consensus-based commentary. The public comment version of The Sedona Conference *Practical In-House Approaches for Cross-Border Discovery and Data Protection* was published for public comment in September 2015 after more than two years of member dialogue, review, and revision, including:

- focus of dialogue during panels at The Sedona Conference International Programmes on Cross-Border Discovery and Data Protection Laws in London, UK, in July 2014 and Hong Kong in June 2015;
- focus of a special WG6 session at The Sedona Conference "All Voices" meeting in New Orleans, LA, USA, in November 2014;
- multiple WG6 member review-and-comment periods; and

- incorporation of comments and feedback from WG6 members representing myriad professions, backgrounds, perspectives, and stakeholders in cross-border discovery and Data Protection Laws.

After nearly a three month public comment period, the editors fully considered and incorporated as appropriate the comments received from the public into this final version.

I thank Katelyn Flynn, Jerami Kemnitz, Cecil Lynn, David Moncure, David Shonka, and Natasha Williams for their diligent efforts and commitments in time and attention to this project. I particularly acknowledge the efforts of Editor-in-Chief Jennifer Hamilton, who shepherded this project through its various stages, and Taylor Hoffman, who led the drafting effort of The Sedona Conference *eDiscovery and Data Protection Model Guideline: Processing & Production of Protected Data in light of Preservation & Disclosure Obligations*, found in Appendix A of this publication.

We continue to welcome comments for consideration in future updates. You are encouraged to submit comments by email to comments@sedonaconference.org.

Craig Weinlein
Executive Director
The Sedona Conference
June 2016

TABLE OF CONTENTS

1. INTRODUCTION

In 2013, a committee[1] of The Sedona Conference Working Group Six (WG6) surveyed selected companies about their experience with cross-border discovery.[2] The committee also interviewed In-House eDiscovery experts about the challenges they face in reconciling U.S. discovery obligations and foreign Data Protection Laws. The committee concluded from the survey and interviews that companies need practical guidance to build on the value of The Sedona Conference *International Principles on Discovery, Disclosure & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation Discovery of Protected Data in U.S. Litigation* ("International Litigation Principles") and The Sedona Conference *Cross-Border Data Safeguarding Process + Transfer Protocol* ("Protocol"), published by The Sedona Conference in December 2011.[3] As a result, the committee prepared this publication, The Sedona Conference

---

1. The Committee on Corporate Outreach would like to extend a special thank you to David Shonka and Katelyn Flynn for their invaluable input and assistance.

2. *See* Jennifer L. Hamilton & Christian Zeunert, In-House Perspective - Practical Experience with Cross-Border Discovery & Data Privacy: Conclusions from the Sedona Conference International Principles Survey & Expert Interviews (2013) (unpublished manuscript) (on file with The Sedona Conference) [hereinafter In-House Perspectives].

3. The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation Discovery of Protected Data in U.S. Litigation*, *available at* https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20International%20Principles%20on%20Discovery%2C%20Disclosure%20%2526%20Data%20Protection [hereinafter International Litigation Principles]. The Sedona Conference *Cross-Border Data Safeguarding Process + Transfer Protocol* [hereinafter Protocol] is included as Appendix C in the International Litigation Principles. Capitalized terms used in this document, and not otherwise defined herein, are defined in the International Litigation Principles.

Practical In-House Approaches for Cross-Border Discovery and Data Protection ("Practical Approaches") to offer solutions to common cross-border challenges.[4] These solutions may not be applicable in all circumstances and practitioners should apply them in good faith and under a standard of reasonableness.

2. IN-HOUSE PERSPECTIVES ON DISCOVERY AND DATA PROTECTION

Discovery and Data Protection Laws vary widely around the world, and these laws may conflict. Therefore, counsel must make choices regarding compliance and create balance to satisfy conflicting obligations.

a. Differing Notions of Privacy

Because member states of the European Economic Area (EEA) follow civil law regimes that differ from the U.S. common law approach and embody vastly different notions about "personal and private" information, they restrict pre-trial discovery and access to information far more than the U.S. For EEA member states, data privacy is a fundamental right, which embraces a much broader view of "personal data" than what generally prevails in the U.S. For example, the 1995 EU Data Protection

4. Companies often address eDiscovery and Privacy functions in different ways. *See* In-House Perspectives, *supra* note 2, at 5. Whereas some In-House litigators may coordinate directly with In-House privacy counsel, eDiscovery counsel may be a one-stop shop for common data protection issues. *Id.* This paper focuses on practical issues for In-House counsel who deal with eDiscovery in coordination with privacy counsel when appropriate.

Directive[5] and similar legislation of each member state[6] protect against the unauthorized processing or transfer of "personal data," which includes any information relating to an identifiable individual.

U.S. concepts of "personal data" and "Processing" of data differ greatly from those in the EEA and many other countries. This difference contributes to difficulties in cross-border communication and collaboration. Similarly, the concept of workplace privacy in the U.S. is often diminished, or even nullified, by the prevalence of computer-use policies that purport to extinguish a worker's right of privacy. In cross-border litigation,[7] this may lead to a misunderstanding of the term "personal data" as it is used in the European Union (EU). The concept of "personal data" in the U.S. is restricted to specific types of personal and sensitive information, such as medical, social security, and banking information. In the EU, this would be considered "personal sensitive information," which commands an even greater degree of protection.

---

5. 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, 1995 O.J. (L 281) 31–50, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML [hereinafter EU Data Protection Directive].

6. It is important to understand that EEA member states implement the EU Data Protection Directive in different ways, and some member states have chosen to give additional protection to personal data. Thus, parties should consider the effect of the laws of the jurisdiction governing processing of any personal data.

7. Although this paper primarily focuses on litigation, many of the practice points and concepts discussed may also be applicable in the context of government investigations and regulatory inquiries. The Sedona Conference has other work product underway that focus on such inquiries.

In the EU Data Protection Directive, the concept of "Processing" is broadly defined as "any operation or set of operations," whether manual or automated, including but not limited to "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[8] In contrast, in the U.S., "Processing" generally relates solely to technical actions specifically related to eDiscovery, such as conversion from one format to another, deduplication, high-level filtering, indexing, and sampling.[9] It is critical to understand these semantic differences in any dialogue regarding these issues.[10]

b. Differing Notions of Discovery or Disclosure

Common law jurisdictions differ from civil law jurisdictions in their litigation procedures, particularly pretrial discovery. Common law practitioners assume that active involvement of individual litigants within an adversarial system is most likely to achieve fair administration of justice. In contrast, civil law practitioners assume that the state, through active participation of an experienced judiciary, is best suited to direct disclosure in the litigant process and protect the privacy of individuals as an inalienable human right. Invariably, the scope of

8. EU Data Protection Directive, *supra* note 5.

9. Even personal data in the hands of third-party contractors and agents is included under the EU Data Protection Directive. *See also* M. James Daley, *Preservation of Electronic Records of Third-Party Contractors*, THE PRACTICAL LITIGATOR (Jan. 2007), *available at* http://files.ali-cle.org/thumbs/datastorage/lacidoirep/articles/PLIT_PLIT0701-Daley_thumb.pdf (U.S. perspective).

10. For more on these issues, *see* International Litigation Principles, *supra* note 3.

permissible pretrial discovery differs dramatically between the U.S. and the rest of the world.

The scope of pretrial discovery in the U.S. is the most expansive of any common law country. The recently revised Federal Rules of Civil Procedure (Fed. R. Civ. P.) generally allow for discovery of "any nonprivileged matter that is relevant to any party's claim or defense and 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 relevant 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. Information within this scope of discovery need not be admissible in evidence to be discoverable."[11] Even with the anticipated benefits of limiting discovery with the Fed. R. Civ. P. Amendments, the U.S. will still be the most expansive discovery regime of any common law country.

In contrast, most civil law countries allow little or no pretrial discovery and do not require any disclosure of evidence beyond what is necessary to prosecute or defend a case. For example, in Germany, litigants are not required to disclose "non-beneficial" documents to the other party. Instead, the parties need only produce those documents that will support its own claims. These documents must be authentic, original, and certified, but the party seeking the document must appeal to the court to order production of the document.

---

11. FED. R. CIV. P. 26(b)(1). The scope of discovery prior to the implementation of the 2015 Amendments was more expansive in that it permitted discovery into any nonprivileged matter "if the discovery appear[ed] reasonably calculated to lead to the discovery of admissible evidence."

Some civil law countries also have enacted blocking statutes to curb the broad reach of discovery from the U.S.[12] For example, in 1980 France criminalized the act of obtaining discovery from France for use in litigation or investigations outside of the country. French Penal Law No. 80-538 provides:

> Subject to international treaties or agreements and laws and regulations in force, it is forbidden for any person to request, seek or communicate, in writing, orally or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature leading to the constitution of evidence with a view to foreign judicial or administrative procedures or in the context of such procedures.[13]

Such statutes are often viewed critically and skeptically by U.S. judges. This can lead to a direct conflict between discovery requirements in the U.S. and data protection obligations outside the U.S.[14]

---

12. *But see In re* Activision Blizzard, Inc. Stockholder Litig., 86 A.3d 531 (Del. Ch. 2014).

13. CODE CIVIL [C. CIV.] art. 1134 (Fr.), CODE PÉNAL [C. PÉN.] art. 111-4 (Fr.), art. 1 bis of law n° 68-678 dated July 26th, 1968, amended by law n° 80-538 dated July 16th, 1980.

14. *See, e.g., In re* Activision Blizzard, Inc. Stockholder Litig., 86 A.3d 531 (Del. Ch. 2014).

3. THE SEDONA CONFERENCE INTERNATIONAL PRINCIPLES ON DISCOVERY, DISCLOSURE & DATA PROTECTION

This document identifies potential approaches to minimizing conflict through the application of the International Litigation Principles.[15] While the International Litigation Principles are advisory and do not carry the force of law, they can:

> provide guidance to public and private parties, counsel, data protection authorities, and the judiciary regarding the management of conflicts that may arise when there is an obligation in one jurisdiction to preserve or produce information from a second jurisdiction in circumstances where the laws of the second jurisdiction may limit the preservation, processing, or transfer of such information.[16]

The Sedona Conference International Principles on Discovery, Disclosure & Data Protection:

Principle 1	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.
Principle 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.

15. International Litigation Principles, *supra* note 3.

16. *Id.* at Preface (v).

Principle 3	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.
Principle 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.
Principle 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.
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.

4. PRACTICE POINTS FOR CONDUCTING CROSS-BORDER DISCOVERY IN VIEW OF DATA PROTECTION AND DATA PRIVACY REGULATIONS

Practice Point #1: Balance the need for urgency in preserving information with the need to proceed deliberately in countries with comprehensive Data Protection Laws.

In order to demonstrate due respect for foreign data protection and privacy laws,[17] *counsel can: (1) identify the cross-border data sources that apply to the matter; (2) diligently research applicable laws that apply to these sources; and (3) confer with specialized Privacy counsel how best to preserve data from these sources in compliance with the law. In-House counsel can balance the enhanced time these processes may require by adopting a preservation plan unique to cross-border discovery matters.*

Hypothetical:

You are employed by a multinational corporation using Model Contract Clauses for transfer of data (instead of Binding Corporate Rules). The company receives a third party subpoena for information relating to the overseas shipment of products manufactured in both the U.S. and the EU. The company retains Outside counsel who has some experience with transferring data out of countries with comprehensive Data Protection Laws and wants to consult with Local counsel in the EU.

Opportunity:

When data sources exist in countries with comprehensive data protection regimes, application of International Litigation Principle 1 suggests counsel should balance speed with "due respect" for foreign Data Protection Laws. Reflexively ordering employees in these countries to preserve all potentially relevant records may trigger a conflict for the employee and company under that country's Data Protection Laws. This can also be confusing to employees who are not accustomed to receiving these types of preservation or legal holds. At the same time, counsel needs to act quickly to identify relevant sources of data to meet

17. International Litigation Principle 1 states that: "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." *See* International Litigation Principles, *supra* note 3, at 7.

U.S. preservation obligations and err on the side of inclusion rather than exclusion.

One practical approach for balancing the urgency to preserve with data protection compliance may be to triage identification and preservation of U.S. data separately from data in the EU, issuing one legal hold notice to U.S. employees separate from EU employees. Prior to or contemporaneously with issuing the EU hold, counsel may consult Privacy counsel to understand the full scope of risk.

Analyzing complex or unfamiliar Data Protection Laws before issuing a legal hold may require more time than may be considered reasonable by a U.S. court, which could lead to sanctions. As a practical matter, counsel may need to consider alternate ways to preserve data outside the U.S. prior to issuing a legal hold notice, such as whether to take snapshots of data and preserve them in the protected country as a backup until the legal hold notice can be issued. Taking this preservation approach will likely constitute processing under EU Data Protection Laws, which will require additional steps to comply with the strict processing requirements.

If a company faces these issues on a recurring basis, it can minimize the risk of a potential lag time by developing and implementing routine internal guidelines based on EU law for processing and production of Protected Data. See Appendix A, *infra*, for an example of such model guidelines. These model guidelines and other documentation may help drive the dialogue with foreign data privacy officials in defense of the process and better inform U.S. courts and Opposing counsel why these additional steps are necessary and important.

Practice Point #2: As early as possible, meet and reach agreements with key stakeholders on a plan that sets expectations regarding legal obligations, roles and responsibilities, and a reasonable timeline.

Early discussions with counsel regarding which documents may be relevant to the matter and where they exist can start a productive dialogue to identify which Data Protection Laws may govern the transfer of data outside the country.

Hypothetical:

You are In-House counsel assigned to a multi-jurisdictional litigation matter and have engaged U.S. counsel. The partner is willing to defer to the In-House procedures as long as it does not slow down investigation of the merits. Outside counsel wants to collect data from Japan and China[18] in the next two to three weeks and is in direct contact with the business team, recommending certain dates for collection.

Opportunity:

International Litigation Principle 2 supports making reasonable decisions when faced with potentially conflicting laws: "[A] party's conduct should be judged by a court or data protection authority under a standard of good faith and reasonableness." This principle encourages counsel to make decisions that compare legal needs with a variety of stakeholder needs, clearly communicate those decisions to the work team, and document the process.

---

18. Japan and China have extensive data protection regulatory schemes. Regarding Japan, *see, e.g.*, Act on the Protection of Personal Information ("APPI") (pending Sept. 2017 amendments); regarding China, *see, e.g.*, Decision of the Standing Committee of the National People's Congress on Strengthening Internet Information Protection (Dec. 28, 2012); Law on Protection of Consumer Rights and Interests (Mar. 15, 2014); Measures for the Punishment of Conduct Infringing the Rights and Interests of Consumers (Mar. 15, 2015); Guideline for Personal Information Protection (Feb. 1, 2013) [not legally binding]; State Secrecy Protection, XIANFA art. 53 (1982); and Law of the People's Republic of China on Guarding State Secrets ("State Secrets Law") (May 1, 1989).

In the hypothetical, the challenge for In-House counsel is to balance these needs with the deadlines that Outside counsel is setting. While Outside counsel may want to focus on the substance of the legal matter, it is important in the beginning stages to get both business and legal buy-in that there are additional considerations that need to factor into decisions like the timeline. The data privacy considerations need to be part of, and in some cases, drive those decisions to achieve the objective in International Litigation Principle 2 of good faith and reasonableness.

The number of internal stakeholders that In-House counsel needs to consult before the case team starts taking action can complicate matters. Here, assume that the legal team recommends arriving in Japan to do a large-scale data collection the week of a national holiday. In addition to complying with U.S. law, it is wise for counsel to consider what effect the timing of a large, in-country collection will have on the business as well as cooperation from the employees at that location. Teaming up with Human Resources may become a high priority to achieve the desired legal outcome. Likewise, for potentially high profile matters, Corporate Communications may need to be consulted about the approach the legal team wants to take.

Furthermore, the issues are complex and difficult to explain to the affected stakeholders on an expedited basis. To gain credibility, In-House counsel may need to circulate the International Litigation Principles to attorneys on the case team. For non-legal stakeholders, summaries in the form of Frequently Asked Questions and visual aids, like infographics, can more quickly build understanding of these issues.[19]

---

19. *See, e.g.*, Appendix C, *infra*, Talking Points Infographic for Internal Business Clients and Employees.

To handle the volume of tasks, In-House counsel may want to use a template case management form.[20] The template case management form can be tailored to the matter and dovetail with court-ordered deadlines and a case management plan. In addition to grouping related tasks, the form formalizes roles and responsibilities. Documentation, like the form, may help support a finding of good faith and reasonableness in the event of a challenge.

Practice Point #3: Identify and define privacy issues with opposing parties or regulators through Outside counsel where possible.

Consider when may be appropriate to start a dialogue on the scope of individual privacy rights and to document any agreement concerning U.S. and non-U.S. obligations.

Hypothetical:

Assume the same facts as the prior hypothetical, but eDiscovery and Privacy counsel are engaged at the earliest stages of the matter.

Opportunity:

International Litigation Principle 4 suggests that seeking a stipulation or court-mandated protective order may help minimize cross-border conflicts and protect personal data.[21] Where possible, counsel may seek such protection to demonstrate to non-U.S. custodians and data protection authorities that reasonable efforts have been taken to protect the confidentiality and

20. *See* Appendix B, *infra*, Template Cross-Border Discovery Management Form for In-House eDiscovery Teams.

21. Protective orders may not be available in the context of responding to a government inquiry or conducting an internal inquiry, but an early dialogue with regulators can foster an understanding that may have a similar effect.

guard against dissemination of personal information. By seeking a stipulation from Opposing counsel or moving the court to issue a protective order, counsel will also have the opportunity to explain the nature and extent of the foreign Data Protection Laws and any legal impediments to producing data from outside the U.S., as well as raise the issues of costs and timing.[22]

The challenge for In-House eDiscovery counsel may not be in ultimately getting this additional stipulation in a protective order, but in convincing either In-House or Outside counsel to introduce the data protection issues to Opposing counsel early enough to negotiate these terms. Outside counsel may be understandably concerned that Opposing counsel will view data protection considerations as pain points to exploit. For this reason, counsel should consider raising data protection issues in early discussions about scheduling orders to avoid having to later contend that it cannot meet its deadlines due to data protection issues. Raising cost issues early can also start the process of building a record with the Court that complying with non-U.S. Data Protection Laws can be expensive and potentially outweigh the value of that data to a particular matter. Proportionality was emphasized during the recent revisions to the Fed. R. Civ. P.: "Parties may obtain discovery . . . that is . . . 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 relevant 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."[23]

---

22. The Model Protective Order in Appendix B of the International Litigation Principles, *supra* note 3, contains a detailed and thorough set of safeguards for counsel to use as a starting point in discussions with Opposing counsel or the court.

23. FED. R. CIV. P. 26(b)(1).

Developing internal, written guidelines that discuss these types of protective orders can help Outside counsel enter into these early negotiations.[24] Furthermore, the process of developing these internal documents will drive the necessary cultural education and behaviors that further underscore Outside stakeholders' confidence that complying with Data Protection Laws is a necessary and achievable part of the discovery process.

Practice Point #4: Set up transparency "checkpoints," beginning with preservation and continuing through the life of the matter, to avoid revocation of consent.

The Article 29 Working Party states in its paper on the interpretation of Article 26(1) that "relying on consent may . . . prove to be a 'false good solution,' simple at first glance but in reality complex and cumbersome."[25] *Consider that consent to transfer may be revoked at any time according to the EU Directive. To minimize that risk, counsel can set up several transparency "checkpoints" throughout the life of the matter, granting custodians an opportunity to understand and agree to the process. Individuals or organizations outside the company may also require periodic notice of the status of proceedings.*

Hypothetical:

During litigation, In-House and Outside counsel discover that an employee located in the EU may have documents

---

24. *See* Appendix A, *infra*, The Sedona Conference, *eDiscovery and Data Protection Model Guideline: Processing & Production of Protected Data in light of Preservation & Disclosure Obligations*.

25. *See* Working document of the Article 29 Working Party on a 'common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995,' WP 114 at 11 (Nov. 25, 2005), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf.

relevant to the matter in the U.S. Outside counsel suggests calling this employee to ask about his documents. In your experience, it is common for Outside counsel to "collect" relevant documents during the course of such a phone call. Outside counsel has no prior experience with foreign Data Protection Laws.

Opportunity:

The hypothetical presents several questions regarding scope of preservation and validity of consent. U.S. parties may be concerned that contacting the employee without first issuing a hold could lead to spoliation. On the other hand, issuing a legal hold before knowing whether the employee has relevant data is the type of overly-broad preservation that may concern relevant EU data protection authorities. In-House counsel also grapple with whether to request consent upon issuing the legal hold or before collecting potentially protected data. Outside counsel may worry that if the employee refuses to consent to preserve, the company is subject to U.S. court sanctions for failing to perform one of its most fundamental tasks during the discovery process.

One approach is to think of gaining consent not as a potential barrier to success but as a way to open the conversation and ultimately gain the trust of employees in data protected countries.[26] The goal is not to achieve a certain number of communications but to confirm and convey that the company and

26. Consent not freely given does not guarantee a legitimate transfer of data. Specifically, it might be difficult to qualify consent as freely given in an employment context, due to the subordinate nature of the relationship between employer and employee. Therefore, the Article 29 Working Party suggests that employers not rely solely on their employees' consent when transferring their data unless they can show that the employees would not suffer any consequences by either withholding their consent or by subsequently withdrawing it. This limitation places a peculiar burden on U.S. defendants with business units in Europe, where a legal matter requires the

counsel will: (1) respect the employee's rights vis-a-vis the company's responsibility; (2) commit to achieving compliance to the best of their ability; and (3) be as transparent as possible about how the company proposes to balance the rights of the employees and the company. Accordingly, providing transparency documents with a request for consent would more fully advance these goals.[27] Furthermore, graphics or diagrams and a detailed collection script may help clarify these steps for employees, who may know nothing about these legal conflicts. Companies that document their efforts to keep employees informed may further demonstrate the reasonableness of the activity under European Data Protection Authority rules.[28]

Transparency can be achieved by other means as well. Full transparency may include giving employees opportunities to review data and confirm their acceptance of transfer of the documents for a cross-border legal matter. This review might occur during the collection interview after counsel explains the issues at stake and identifies personal data that does not need to be collected. Counsel may also provide employees with an opportunity to review personal folders or emails and remove them

---

company to transfer documents with personally identifiable information across national borders. Although consent of employees may not suffice as an independent basis for transferring private data, transparency throughout the life of the matter may resolve most employee concerns about what will happen with their data and minimizes the risk that employees will subsequently withdraw their consent. *See also* In-House Perspectives, *supra* note 2.

27. Consider whether transparency documents require translation for the recipients, depending on legal requirements and the employee's fluency in a particular business unit.

28. International Litigation Principle 5 states: "[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." International Litigation Principles, *supra* note 3, at 19.

from the collection process. Furthermore, some companies have given employees the opportunity to conduct their own privacy review after the company collects documents and before transfer or production of the data. These transparency steps, in addition to obtaining consent, may achieve the company's objective of compliance with legal obligations as well as data protection and privacy laws, while satisfying key stakeholders in the process—the employees. Full transparency may pose a significant challenge in larger matters with lots of custodians. Counsel may need to find alternative ways to avoid increasing burden and expense in achieving transparency.

Practice Point #5: Plan a successful in-country collection with detailed surveys of appropriate systems well in advance, and by soliciting support from key stakeholders, both in corporate departments and local business units.

Counsel can reduce the expense and risk of in-country collections by learning about key stakeholders, key systems, and country customs. The logistics involved should be planned in detail as soon as counsel knows that he or she must collect information from any non-U.S. country.

Hypothetical:

After an in-country data collection commences, the Information Technology (IT) department discloses that the server where the EU employee saves data is shared with non-company business units located in the same industrial business park.

Opportunity:

International Litigation Principle 3 states that "[p]reservation 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."[29] Planning for a targeted collection may help balance conflicting interests. Even so, there is much work to be done prior to an in-country collection, starting with identifying key IT contacts in the targeted locations.

In the hypothetical, after counsel discovered that key servers were "shared" with other businesses, counsel may want to identify the right people to engage at these other businesses. For example, counsel would probably want to consider: (1) whether to contact the Chief Executive Officer or the Chief Information Officer; (2) who has the authority to sign any type of transparency or consent form to permit access to the data at other companies using the servers; and (3) the requirements counsel must follow to minimize the risk of infringing on data protection and privacy laws.[30]

In addition, this scenario points to the value, as identified under Practice Point #1, of having a plan in place before discovery issues even arise. Next time, before commencing collection, counsel may want to conduct surveys of systems that potentially store relevant data. Such surveys typically include: (1) the key witnesses; (2) the business owners; and (3) any IT owners of the systems. This reduces the chance of learning too late that several independent companies share the same file servers.

---

29. Recall that the European privacy model encourages limiting the collection to what is necessary to the matter rather than employing a "take it all now, figure it out later" approach.

30. Of course, in an ideal situation, counsel would have been aware of the shared servers prior to litigation or an investigation. As a practical matter, this is not always the situation despite good faith diligence of counsel.

Practice Point #6: Use the Processing stage of discovery as an opportunity to balance compliance with both discovery and Data Protection Laws, thereby demonstrating due respect for Data Subjects' privacy rights.

Early discussions regarding data Processing can address requirements related to both Data Protection Laws and local court procedures and demonstrate due respect to any Data Subject with rights under applicable Data Protection Laws.

Hypothetical:

In-House and Outside counsel meet to determine the best way to cull and filter the large amount of collected data. They do not ask a business representative to join this meeting. Outside counsel wants to use a U.S.-based vendor to process the data because of the preferred rates offered by the vendor's local office.

Opportunity:

After collecting information potentially relevant to a lawsuit or investigation, organizations must "process" that information before producing it. "Processing," as used in U.S. eDiscovery, is the automated ingestion of electronically stored information (ESI) into a program to extract metadata and text and create a static image of the source ESI according to a predetermined set of specifications, in anticipation of loading the information into a database for review. Processing specifications may include filtering data based on metadata or full text contents to include or exclude the results of such filtering in the final work product for review.

The Processing stage is an opportunity under the International Litigation Principles to protect privacy while complying with discovery obligations. International Litigation Principle 3 states, in part, that "discovery of Protected Data should be limited in scope to that which is relevant and necessary to sup-

port any party's claim or defense." Before Processing any collected data, counsel may want to meet with key business representatives and learn the business language that relates to the pending legal matter. After learning relevant business terms, names, and dates, a keyword search list can be developed to help eliminate irrelevant information from the data set. Decisions made throughout this process should be documented, pursuant to International Litigation Principle 5, to demonstrate reasonableness and due respect for data protection obligations. The search process should be iterative, and the results should be continuously analyzed by counsel and revised as necessary.

Counsel can include terms and set parameters that will help identify Protected Data. For example, the names of financial institutions may help isolate an individual's banking records that he or she has kept in an email or document files. Similarly, unless the employee has used his or her personal email to conduct company business, email domain addresses often associated with personal emails, such as hotmail.com or gmail.com, may be isolated to help identify non-work related communications for removal from the potentially relevant data set.

The Processing phase also serves as a key decision point regarding the transfer of data out of the country from which it was collected. Under International Litigation Principles 1 and 2, parties may try to perform culling and filtering exercises in the country where the data was collected so irrelevant Protected Data can be removed from the data set prior to transfer. If data must be transferred out of country for review, an initial culling before transferring the information may help demonstrate respect for local Data Protection Laws while complying with any conflicting discovery obligations outside the country. Parties should take advantage of technological advances and the ability to perform processing activities nearly anywhere in the world to balance privacy rights with disclosure obligations.

Practice Point #7: During review of data for production and disclosure, parties may consider ways to limit the production of Protected Data; when production of Protected Data is necessary, safeguards can be established to demonstrate due respect for both discovery and Data Protection Laws.

The review and production stages may be used to protect privacy interests of the Data Subjects whose data has been collected for use in the legal matter. The Model Protective Order in Appendix B of the International Litigation Principles provides one way to balance discovery and disclosure obligations with individual data protection rights.

Hypothetical:

Hundreds of thousands of documents remain in the data set after culling and filtering. Outside counsel wants to use its U.S. based associates to perform a linear document-by-document review of the material. In-House counsel usually employs a document review vendor that has facilities throughout the world and uses a review platform that includes the latest technology assisted review functionality. Before Outside counsel meets with Opposing counsel to discuss production formats and timelines, In-House and Outside counsel meet to develop document review guidelines and to set parameters around production.

Opportunity:

After culling and filtering the data set, parties generally perform some level of "eyes on" review of the documents before production to Opposing counsel. Document review may range from a high level spot check of a sample of the collected and filtered data to a full document-by-document review of every item in the data set. The goal of review is to isolate and produce only that information which is relevant to the claims or defenses of a party.

One key decision is whether to review data in the country in which it was collected ("in-country review") or, if in-country

review is not possible, in a country with similar Data Protection Laws ("near-country review"—a distinction based on regulatory rather than geographic proximity). Accordingly, an "eyes on" review in- or near- country may further demonstrate compliance with Data Protection Laws, creating an added safeguard against the production of non-responsive Protected Data while balancing the need for production with the protection of individual privacy rights. See International Litigation Principles 1, 2, and 3.

Parties may wish to consult with Local Privacy counsel, Outside eDiscovery counsel, and technology vendors to consider additional available review options and to ensure they are both technologically feasible and, more importantly, compliant with local data privacy regulations.

In-House and Outside counsel should consider drafting document review guidelines (DRGs) for attorneys performing the review. These DRGs may include protocols for tagging documents with Protected Data—particularly non-responsive documents that may contain Protected Data. For example, among the responsive/non-responsive issue tags, counsel may include tags labeled "responsive – personal data" and "non-responsive – personal data." This will allow counsel to determine the volume of "responsive – personal data" and formulate a disclosure plan. One benefit of tagging "non-responsive – personal data" is that if a large amount of "non-responsive - personal data" is identified in the initial collection(s), collection criteria could be modified to minimize the amount of such data in any subsequent collections.

If Protected Data must be produced to Opposing counsel, the responding party should consider safeguards to limit production of such data, such as producing data in an anonymized or redacted format. For example, an employee roster that iden-

tifies all workers on a particular project may have multiple columns of Protected Data, including name, address, phone number, personal identification numbers (PINs), and nationality. If this document must be produced, PINs could be redacted, and addresses and phone numbers could be anonymized to include one single business address and phone number. The nationality field might also be aggregated to show only the number of workers representing each nationality. Anonymization, pseudonymization, redaction, and aggregation are often applied to productions if required by local laws/regulations and are consistent with the guidance of International Litigation Principles 1, 2, and 3.

Tiered or staged productions offer another method of limiting the production of Protected Data. Oftentimes, employees maintain duplicative, or nearly duplicative, emails and project files. To balance data protection rights with discovery obligations, parties may agree to review U.S. productions first. Afterwards, the parties may be able to agree that further production from non-U.S. custodians is not necessary. If further production is necessary, parties might agree on an extended review and production timeline to accommodate the additional time needed to review and produce data from outside the U.S.

To protect responsive data containing Protected Data that must be produced, parties can agree on a protective order similar to the Model Protective Order in Appendix B of the International Litigation Principles.[31] As International Litigation Principle 4 states, "where a conflict exists between Data Protection Laws and preservation, disclosure, or discovery obligations, a stipulation or court order should be employed to protect

31. *See* International Litigation Principles, *supra* note 3, at Appendix B. Note, however, that such stipulations and protective orders are usually not available in government investigations.

Protected Data and minimize the conflict." Such an agreement can be used, for example, to limit the number of people allowed to view the Protected Data, and impose immediate destruction requirements on Protected Data, as detailed in International Litigation Principle 6, either after that information is reviewed by the requesting party or as soon as it is no longer needed for the matter.

Practice Point #8: To avoid keeping data longer than necessary, counsel should prepare to release legal holds and return or dispose of data promptly upon termination of a matter.

Once a matter is concluded, legal holds may be released and data returned or disposed of depending on its retention requirements. A matter is fully concluded when, for example: (1) a final settlement agreement and release has been signed by all parties; (2) a dismissal with prejudice has been entered as to all parties and the deadline for any appeals has run; (3) any judgment has become final; or (4) in government investigations, when the government has indicated that the investigation has been concluded, for example, through a letter of declination, return of documents, or any other formal notice of the conclusion of the investigation.[32]

Hypothetical:

The U.S. Litigation involving the employee in the EU has settled and the data collected is no longer needed for litigation or other purposes. However, the company would like to keep the data in the event that similar, although unanticipated, claims arise in the future. The company is primarily motivated by the high cost and significant amount of time required to retrieve

32. Under Fed. R. Civ. P. 52(b) a party has 28 days to move the court to make additional findings or amend its findings or judgement. Under Fed. R. Civ. P. 59, a party has 28 days to seek a new trial.

and search the data and engage Outside counsel to navigate potential privacy issues with regulators and Opposing counsel. The company's primary argument for retaining the data is that all personal data should have been purged during EU-based document review prior to its transfer and the company would rather have this information available should it need the data again in litigation.

Opportunity:

As noted in International Litigation Principle 6, "[o]rganizations should take good faith, reasonable efforts to retain, manage, and dispose of inactive data both on a prospective and retrospective basis." This approach comports with the European data protection authorities' preference for "data minimization," as the less personal data collected or retained by an organization, the lower the cost and risk associated with data protection. This approach also supports sound records management practices, which have been interrupted by imposition of preservation steps taken in connection with the legal action.

Throughout the proceeding, In-House counsel should maintain a record, or inventory, of all locations where data is preserved, collected, or produced during the matter, whether it is stored on the company's U.S. server; or with Outside counsel, third party vendors, or opposing parties and their vendors. At the end of the matter, counsel may use this inventory to seek return of the data or otherwise certify its disposal in accordance with its discovery protocols. By doing so, counsel will demonstrate compliance with foreign Data Protection Laws and also build a record that will provide insights for the company in future actions.

While counsel may prefer to retain indefinitely all EU data that has been legitimately transferred to the U.S. for litigation purposes, doing so would contravene International Litigation Principle 6 as well as the EU Directive. The EU Directive

provides that Protected Data should be retained only as long as necessary to satisfy legal or business needs. The company's purported business need (i.e., the high cost of obtaining the data weighed against the possibility of future litigation) would appear to be outweighed by the privacy rights of non-U.S. citizens under the EU's strong policy of protecting personal data. Moreover, the company's assertion that all personal data related to the EU employee (and others) was removed "in-country" largely ignores the probability that some personal data may have remained in the production due to its relevance to the subject matter of the litigation. The argument also ignores the fact that prior to production of the personal data, the litigation parties may have entered into confidentiality agreements or a protective order dictating appropriate use and disposal of the data.

The company is responsible for ensuring the return or disposal of personal data. Post-litigation disposition of personal data comports with International Litigation Principle 6 and prior Commentary.[33] Prompt disposal of data also provides assurance to non-U.S. data protection and privacy authorities that U.S. companies enforce legitimate preservation obligations rather than collect information based on a legal action that may occur in the future.

5. CONCLUSION

Cross-border discovery presents a growing challenge for courts, privacy authorities, companies, employees, counsel, and requesting parties. Practical solutions are necessary to reconcile potentially conflicting obligations in a reasonable manner. This Practical Approaches document is one additional step to achieve these solutions.

---

33. *See, e.g.*, The Sedona Conference, *Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265, 259 (2010).

6. PRACTICAL APPROACHES APPENDICES: THE SEDONA CONFERENCE IN-HOUSE TOOL KIT FOR DATA PROTECTION AND CROSS-BORDER DISCOVERY

The tools in the following appendices were designed to help companies approach cross-border discovery and Data Protection Laws on a practical level. Developing a set of internal tools for cross-border discovery is not a small task and not every company will have the need or resources to do so. However, the process of developing even one of these tools results in more than just guidance on future legal matters. It forces key stakeholders to educate each other about important legal and cultural considerations; to grapple with philosophical issues and make proactive decisions; and to develop a network of internal contacts that can act quickly when these situations arise. The education alone that the stakeholders receive may be worth the effort, even more so where the company has locations in multiple jurisdictions around the world or faces these issues on a regular basis.

A. The Sedona Conference eDiscovery and Data Protection Model Guideline: Processing & Production of Protected Data in light of Preservation & Disclosure Obligations

B. Template Cross-Border Discovery Management Form for In-House eDiscovery Teams

C. Talking Points Infographic for Internal Business Clients and Employees

D. Exemplar Heat Map of Data Protection and Data Privacy Regulations

APPENDIX A: THE SEDONA CONFERENCE eDISCOVERY AND DATA PROTECTION MODEL GUIDELINE: PROCESSING & PRODUCTION OF PROTECTED DATA IN LIGHT OF PRESERVATION & DISCLOSURE OBLIGATIONS

What it is: A customizable roadmap describing steps a company may take to minimize potential conflict of eDiscovery and Data Protection Laws in line with the International Litigation Principles.

Who it is for: In-House counsel, eDiscovery Team, privacy officers, and Outside counsel.

Why it is important: Provides consistent basis to approach individualized matters and demonstrates reasonableness and good faith.

How to use it: To be applied in conjunction with the company's policies to legitimize company processes and educate stakeholders for matters that may require significant resources.

Appendix A Table of Contents

Preface

In 2013, The Sedona Conference (TSC) formally launched the Committee on Corporate Outreach of Working Group Six on International Electronic Information Management, Discovery, and Disclosure (WG6). The committee's mandate is an important one, i.e., strengthening the practical applicability of The Sedona Conference *International Principles on Discovery, Disclosure & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation Discovery of Protected Data in U.S. Litigation* ("International Litigation Principles"). In its first year, the committee conducted its first annual TSC International Principles Survey, reporting the results for In-House eDiscovery and data protection experts and underscoring the need for practical guidance for In-House eDiscovery experts, including a need for materials such as an eDiscovery and Data Protection Model Guideline. This Sedona Conference *eDiscovery and Data Protection Model Guideline: Processing & Production of Protected Data in light of Preservation & Disclosure Obligations* ("Guideline" or "Model Guideline") is one of the tools included in the appendix to the *Practical In-House Approaches for Cross-Border Discovery & Data Protection* document ("Practical Approaches").

Each section of this Guideline includes model guideline language and a comment section. The Guideline language contains building blocks corporations can use for their In-House guidelines, recognizing the potential need to modify the language given the individual corporation's circumstances (e.g., industry, countries of operation, cultural specifics). The comment sections highlight key issues as well as potential areas of modification. It does not, however, attempt to address all potential considerations for modification.

1. Introduction/Guideline Purpose:

Model Guideline Language

The Sedona Conference *eDiscovery and Data Protection Model Guideline: Processing & Production of Protected Data in light of Preservation & Disclosure Obligations* ("Guideline" or "Model Guideline") provides guidance for Company to address both its U.S. eDiscovery and non-U.S. data protection obligations during litigation in the U.S. and to minimize any potential legal cross-border conflicts arising between the two.[34] By applying this Guideline under a standard of reasonableness and good faith, potential conflicts can be minimized. The Guideline is not meant to be a step-by-step manual and may not be appropriate or applicable in every matter. The assigned In-House counsel should consult on specific matters as needed with eDiscovery counsel/team and appropriate Company Data Protection Officer (DPO).

This Guideline is to be applied in conjunction with Company's Group Data Protection Policy and other relevant policies.

Comment

This Model Guideline focuses on U.S. eDiscovery and non-U.S. data protection obligations.[35] Companies may need to

34. While the Guideline and companion FAQ have been crafted to address data protection issues in the context of litigation, Company may consider leveraging them in part to address transactional and compliance-related uses of protected Company data. Please note that WG6 anticipates preparing an additional Guideline and companion FAQ to address internal and government investigations in conjunction with a related WG6 public comment publication that is in the process of being finalized.

35. Non-U.S. data protection obligations include data privacy obligations as covered by the EU Data Directive (and the laws enacted by its member states or other countries that have modelled their data protection

consider including more tailored language for the various regions/countries at issue and/or providing more specific guidance regarding country-specific issues (e.g., blocking statutes or relevant penal codes), depending on the circumstances. In addition, companies may want to clarify specific privacy issues depending on the Company's industry and the regulatory environment in which it operates (e.g., banking consumer data or medical data). In addition to modifying the Model Guideline scope, companies may want to specify the goal(s) of their guideline. For example, some companies may want to streamline an approved process for "standard" matters and define parameters for "exceptional" matters. Others may focus their intent on building a consistent approach.

Companies must also determine how best to internally market or roll out their guideline. A guideline introduced without sufficient internal buy-in and education faces greater challenges in being consistently implemented. The corresponding FAQ to the Model Guideline provides examples of questions which may arise for employees who are not frequent practitioners of cross-border discovery but may benefit from guidance and big-picture issue flagging. Obviously, they should be modified both in scope and specificity depending on the company's needs.

2. Principles:

Model Guideline Language

This Guideline incorporates, where appropriate, the *International Principles on Discovery, Disclosure and Data Protection: Best Practices, Recommendations & Principles for Addressing the*

schemes on the EU Directive), state secrecy laws as found in China, banking secrecy laws such as those found in Switzerland, to name a few.

Preservation Discovery of Protected Data in U.S. Litigation ("International Litigation Principles"), published by The Sedona Conference in December 2011.[36] While the International Litigation Principles are advisory and do not carry the force of law, they are intended to provide guidance to public and private parties, counsel, data protection authorities, and the judiciary regarding the management of conflicts that may arise when there is an obligation in one jurisdiction to preserve or produce information from a second jurisdiction in circumstances where the laws of the second jurisdiction may limit the preservation, processing, or transfer of such information. Capitalized terms used in this Guideline, and not otherwise defined herein, are defined in the International Litigation Principles.

The Sedona Conference International Principles on Discovery, Disclosure & Data Protection

Principle 1	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.
Principle 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

36. The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation Discovery of Protected Data in U.S. Litigation*, *available at* https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20International%20Principles%20on%20Discovery%2C%20Disclosure%20%2526%20Data%20Protection [hereinafter International Litigation Principles].

data protection authority under a standard of good faith and reasonableness.

Principle 3 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.

Principle 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.

Principle 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.

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 Model Guideline includes all of the International Litigation Principles in a separate section here because they are cited throughout the Model Guideline and provide its foundation. However, for purposes of length, companies may consider merely incorporating them by reference or including the specific

International Litigation Principles throughout the guideline when applicable.

3. Intended Audience and Case Kick-off:

Model Guideline Language

The intended audience for this Guideline is Company's internal personnel in Legal, IT, Compliance and other functions who manage legal proceedings involving U.S. eDiscovery and non-U.S. Protected Data.

To ensure that data preservation, collection, hosting, review, and production are performed consistently and to minimize potential conflicts between Company's U.S. eDiscovery and non-U.S. data protection obligations, the eDiscovery Team must be consulted in all eDiscovery matters involving non-U.S. data.

For each specific matter, the relevant Company DPO, In-House Litigation counsel, In-House eDiscovery counsel, and eDiscovery project manager should consult on the relevant sources of data and custodians, as well as which regional/country-specific data regulation applies to each data source and custodian. At this early stage, these individuals should also begin to address issues to be raised with Opposing counsel in a subsequent meet-and-confer (e.g., potential protective orders, whether a Hague Convention request or letters rogatory may be needed, etc.). Each of these individuals brings specific knowledge and skill sets that will assist the Company in complying with both its U.S. eDiscovery and non-U.S. data protection obligations, and in minimizing any potential legal cross-border conflicts arising between the two.

Comment

Companies should modify this language to reflect their organizational structure and naming conventions (for example,

some smaller companies with limited litigation profiles may not even have an In-House dedicated eDiscovery Team). However, companies should only exclude a functional equivalent of any of the above-named roles (i.e., personnel in Legal, IT, Compliance, and other functions who manage legal proceedings involving U.S. discovery and non-U.S. Protected Data) after careful consideration. These roles should consult and come to agreement on the guideline and specific processes and procedures prior to a specific matter arising requiring U.S. discovery of non-U.S. Protected Data. Again, depending on regional and national scope, and the domestic regulatory environment, regional or local roles should also be consulted (e.g., a Company DPO specializing in Protected Data residing in Asia). Broad stakeholder buy-in at the time of implementation is key to ensure that the guideline is followed consistently across various lines of business or internal Company silos and does not create conflicts with existing Company policies that may otherwise overlap with the guideline.

On a per-matter basis, companies may consider whether it is necessary to consult all of these functional roles and instead delegate to a subset after all of the functional roles have approved an overall process. If these functional roles are not included on a per-matter basis, they should regularly consult to ensure that the approved processes and procedures are still appropriate. Moreover, individuals handling specific matters should consult frequently and raise any unusual circumstances or unfounded assumptions.

The Model Guideline references the meet-and-confer with Opposing counsel at an early stage in the spirit of TSC's *Cooperation Proclamation*,[37] and because early communication of

37. The Sedona Conference, *Cooperation Proclamation*, 10 SEDONA CONF. J. 331 (2009 Supp.).

potential cross-border transfer concerns can minimize subsequent disputes among parties.

4. Preservation (Legal Hold) Process and Data Protection Safeguards:

Model Guideline Language

In the U.S., parties are required to identify, locate, and preserve data that is potentially relevant to pending or reasonably anticipated U.S. Litigation. This duty is rooted in the U.S. common law requirement to avoid spoliation of relevant evidence.[38] Non-U.S. data protection regulations, on the other hand, define this preservation as "Processing" even if the Protected Data is not transferred, creating a potential tension between the two regulatory regimes. The process outlined below provides a framework for Company to comply with its preservation obligations while also taking account of appropriate non-U.S. data protection safeguards.

a. Scoping and Data Minimization

Data minimization, i.e., preserving only the data potentially relevant to any party's claim or defense, is an effective data protection safeguard.[39]

The scope of a Legal Hold should be determined at the direction of counsel and in compliance with applicable preservation obligations. In light of the data minimization safeguard,

---

38. The Sedona Conference, *Commentary on Legal Holds: The Trigger and The Process*, 11 SEDONA CONF. J. 265 (2010).

39. *See* International Litigation Principles, *supra* note 36, Principle 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.").

the Legal Hold should be appropriately limited with respect to the (1) data custodians (i.e., the individuals placed on hold), (2) data categories, and (3) relevant time frame.

Scoping and data minimization does not conclude with the initial Legal Hold but instead is an iterative process. As the matter evolves (e.g., through an amended complaint or a better understanding of the facts based on custodian interviews), the scope of the Legal Hold should be appropriately adjusted.

b. Transparency and Employee Acknowledgement

Transparency, i.e., taking reasonable steps to notify non-U.S. Data Subjects of the purpose(s) for which their personal data may be processed, is also an effective data protection safeguard.[40] Company is not required to seek notification and/or consent where it is prohibited by law or where an exception is provided by law.

The Legal Hold Notice issued to non-U.S. Data Subjects should explain the purpose, scope of information to be preserved, potential subsequent use of preserved information, and potential consequences of not preserving relevant information. In addition, the Legal Hold Notice should include a notice of rights to access, modify, and oppose processing of personal data. Transparency, in addition to being good data protection practice, reduces opposition from custodians throughout the discovery process.

---

40. *See* International Litigation Principles, *supra* note 36, Principle 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.").

For current employees, the standard language in a Legal Hold Notice may request confirmation from non-U.S. data custodians[41] that they understand the Legal Hold and potential data protection implications. Company obtains consent from non-U.S. employees departing Company as part of the off-boarding process.[42] In instances in which it becomes known that a non-U.S. former employee has not provided consent, Company will take reasonable steps to contact the individual using last known contact information. Depending on the country of the custodian, it may be appropriate for Company to offer the non-U.S. data custodian an opportunity to assess and limit the potential privacy impact by reviewing and tagging as "private" certain communications. In-House Litigation counsel, In-House eDiscovery counsel, the relevant Company DPO, and any applicable body such as a Company Works Council in Germany, or the local data protection authority (DPA), such as the National Commission on Informatics and Liberty (CNIL) in France or the Information Commissioner's Office (ICO) in England and Wales, will address how to proceed with respect to any country-specific requirements if a conflict arises between the interests of the non-U.S. data custodian and Company.

41. A "data custodian" refers to the employee whose mailbox is collected in contrast to a "Data Subject," which more broadly refers to an individual whose personal data may be included in data custodian's mailbox. Obviously, it is often impractical to obtain consent from every Data Subject and, thus, Company should undertake other appropriate safeguards in furtherance of Principle 3.

42. While not all data protection authorities may view consent as sufficient, consent nevertheless furthers the goal of transparency.

c. Legal Hold Release and Data Disposal

Releasing Legal Holds and disposing of data that is subject to the corresponding Legal Holds are effective data protection safeguards.[43] Company's preservation obligation is limited in duration to the time during which a legal action is pending or remains reasonably anticipated.

At the conclusion of a matter (e.g., when the applicable time period for appeal has expired or litigation is no longer reasonably anticipated), Company provides employees subject to the Legal Hold with a written Legal Hold Release Notice. If the Protected Data is not subject to another Legal Hold, it is then maintained according to applicable records retention guidelines. With appropriate consultation with In-House counsel and the Records Management Group, the Protected Data previously subject to a Legal Hold will be destroyed under the management of the eDiscovery Team if (1) the applicable records retention schedule has expired; (2) the Protected Data is not subject to another Legal Hold or other legal obligation; and (3) there is no other valid reason to maintain the Protected Data (e.g., business requirement).

Comment

This Model Guideline language highlights the inherent tension between U.S. preservation obligations and the non-U.S. definition of "Processing." Even ideal circumstances (consent from the data custodian and approval from the Company DPO

43. *See* International Litigation Principles, *supra* note 36, 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."); s*ee also* International Litigation Principles, *supra* note 36, Principle 3 regarding data minimization.

and applicable Works Council) raise preservation concerns given timing and logistics.

Appropriate scoping and data minimization are clearly important aspects of limiting data protection implications. Interviewing subject matter experts and identified custodians helps to ensure that Company strikes the right balance. In fact, it may come to light that named custodians do not, in fact, have relevant data and can be removed from the Legal Hold.

This Model Guideline language also acknowledges that not all Works Councils nor Company DPOs may find consent and transparency sufficient. In these matters, the In-House litigator, In-House eDiscovery attorney, relevant Company DPO, and Works Council should consult to find a mutually agreeable solution and—importantly—weigh the costs and benefits of not complying with U.S. eDiscovery obligations. It is advisable in most cases (and especially in cases in which the custodian denies consent) to consult with the subject matter experts and custodians to determine whether there is substantively duplicative data that has lesser data protection concerns.

While the Model Guideline suggests that consent and transparency be included in the Legal Hold Notice, it is also an acceptable practice for this to be included in a separate communication with the data custodians. Regardless of which document this communication resides in, it should include contact information for any potential follow-up questions.

This Model Guideline proposes that the Company provide the Data Subject with the opportunity, at his or her request, to conduct a privacy review. This raises the potential for misuse of the privacy review (e.g., the data custodian using the privacy review and redaction process to hide his or her own malfeasance rather than culling legitimately private information (such as medical data)). If there is reason to suspect this, the applicable Company DPO, Works Council, In-House litigator, In-House

eDiscovery counsel, and In-House Human Resources counsel should consult on an appropriate action.

Finally, the conclusion of a matter provides an important data protection step often overlooked by In-House and Outside counsel. Company should consider including the steps described in this Model Guideline in any applicable case closeout checklist.

5. Post-Preservation Process and Data Protection Safeguards:

Model Guideline Language

The eDiscovery process requires additional data protection safeguards beyond the preservation stage (i.e., collection, processing, hosting, transfer, review, and possible production). The process outlined below provides a framework for Company to comply with its discovery obligations with appropriate non-U.S. data protection safeguards.

a. Initial Case Assessment on Data Protection Implications

Each matter may involve data from a number of jurisdictions for which applicable Data Protection Laws need to be considered.[44] Therefore, at the outset of each matter, In-House counsel and a member of the eDiscovery Team should consult to identify the country scope for identified data collections (i.e., the countries where information is located) and appropriate data

44. *See* International Litigation Principles, *supra* note 36, Principle 1 ("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.").

protection safeguards, including potential cross-border data restrictions.

In some circumstances, Company may be required to consult the local DPA or the Company Works Council, and even take into account criminal statutes (e.g., Swiss Penal Code Articles 271 and 273), blocking statutes (e.g., France and Switzerland), or industry specific restrictions (e.g., banking secrecy laws).

Moreover, whether notification or approval of a DPA is required depends upon the local Data Protection Law and certain factors, including: the mechanism chosen for legitimizing the transfer of Protected Data to the United States; whether it concerns a single or repeated transfer; and the amount of data to be transferred. On one end of the spectrum, for example in Belgium or the UK, DPA approval may not be required, provided that the receiving party (e.g., eDiscovery service provider or Retained counsel) is either Privacy Shield certified or has executed Standard Contractual Clauses. However, further onward transfers to third-parties (e.g., opposing party or the court) may require other safeguards like a protective order with appropriate data protection language. On the other end of the spectrum, for example in France or Spain, DPA notification or approval may be required.

If the data has already been transferred to a recipient in the U.S., onward transfer to a third-party recipient in the U.S. (usually the opposing party in U.S. Litigation) is legitimate through a "stipulative court order" (or presumably a protective order), specifically addressing certain data protection criteria (e.g., confidentiality, security, access, restricted use, and distribution). In such cases, the onward transfer requires neither formal approval from nor notification to the DPA. However, the exporting party should be prepared to provide a copy of the protective order in the event of an audit by the DPA. Protective

orders alone, however, may not be an adequate basis for the initial transfer of data to the U.S.

The eDiscovery Team should also determine whether it is appropriate to provide post-preservation notice and/or consent to current and former non-U.S. employees who are data custodians as the eDiscovery process continues. As described above, former employees provide consent as part of the off-boarding procedure. In instances in which it becomes known that a former employee has not consented, Company will take reasonable steps to contact the data custodian using last known contact information. If Company is unable to do so, the eDiscovery Team should consult the Company DPO, In-House counsel, and any other applicable data protection authority such as the Works Council (in Germany) or the CNIL (in France). Again, it is unreasonable to obtain consent from Data Subjects as opposed to data custodians and, thus, Company should undertake other appropriate safeguards in furtherance of International Litigation Principle 3.

As part of case management, the eDiscovery Team should document steps taken to safeguard data protection.[45]

b. Collection, Hosting, Review, and Production

Data minimization is also an effective data protection safeguard at the collection phase.[46] In-House counsel and an eDiscovery Team member should consult regarding search

45. *See* International Litigation Principles, *supra* note 36, Principle 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.").

46. *See* International Litigation Principles, *supra* note 36, Principle 3 regarding data minimization.

terms and time period. Adhering to the U.S. principle of proportionality[47] furthers this safeguard by limiting the overall scope of discovery.[48]

The use of an internal analysis and hosting tool housed and managed in-country or in-region is an effective data protection safeguard. This minimizes the need for cross-border transfer of Protected Data and reduces data security risks. Obviously, there are many circumstances in which it is not practical or feasible for non-U.S. Protected Data to remain on Company's internal tool (e.g., data transfer to Outside counsel or remote access to the internal tool provided to Outside counsel or eDiscovery service provider outside the region). In these circumstances, the eDiscovery Team should consult, as applicable, the Company DPO, Works Council, and/or local data protection authority, and implement additional safeguards (e.g., Privacy Shield certification, execution of Standard Contractual Clauses, inclusion of data protection language in the engagement letter, assurance of secure authentication for access to a limited and identified list of individuals, and prohibition of batch print function).

It may be appropriate for Outside counsel to seek an agreement with Opposing counsel or seek to obtain a court order permitting phased productions to provide Company additional time to implement appropriate safeguards for non-U.S. Protected Data. If production of non-U.S. data is required but presents a conflict with non-U.S. Data Protection Laws, a protective order limiting dissemination and preservation duration

47. *See* FED. R. CIV. P. 26(b)(2)(C) and 26(g)(1)(B)(iii).

48. The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 14 SEDONA CONF. J. 155 (2013), provides additional guidance on this principle.

of the Protected Data may be an appropriate safeguard.[49] Redactions and/or anonymizations may also be appropriate safeguards, although they may not be practical or permitted in certain circumstances.

c. Case Closure and Data Disposal

Ensuring proper disposal of data at the conclusion of a matter is an effective data protection safeguard.[50] The eDiscovery Team should consult with In-House counsel to determine whether it would be appropriate and feasible to obtain certifications of destruction (or other means of confirmation) from Outside counsel, vendors, and Opposing counsel.

Comment

Section a., Initial Case Assessment on Data Protection Implications, of this Model Guideline focuses on specific data protection regulations. This, clearly, is ripe for modification depending on the Company's specific circumstances. However, the Company should be careful to not merely delete potential inapplicable regulations but should instead consult with the Company's counsel to address whether additional specific data protection regulations (whether they be country- or industry-specific) should be addressed here. The Company should also

---

49. *See* International Litigation Principles, *supra* note 36, Principle 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.").

50. *See* International Litigation Principles, *supra* note 36, 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.").

consider whether internal policies on data handling impacts certain data protection regulations; for example, permitting private use of a Company's email system may affect other regulations, e.g., the German Telecommunications Act.

This Model Guideline also suggests that the eDiscovery Team document steps taken to safeguard data protection. Regardless of which functional entity the Company tasks with this responsibility, it should be clearly defined to help ensure that a potential demonstration of steps taken is centrally located. The level of detail may appropriately vary company-by-company.

Regarding the hosting and management of the hosting tool, it is important to consider the jurisdictions of who has access and/or permissions to grant access. A hosting tool physically located within the region may be better than being physically hosted in the U.S., but it provides greatly reduced protection if it is managed and/or accessible to U.S.-based personnel. It may also be appropriate to inform document reviewers of country- or region-specific Data Protection Laws that may affect the review and also implement additional safeguards. For example, if search terms return a clearly private email, it may be appropriate to delete it from the review platform rather than merely coding the document as non-responsive.

Again, the conclusion of a matter provides an important data protection step often over looked by In-House and Outside counsel. Company should consider including the steps described in this Model Guideline in any applicable case closeout checklist.

6. Conclusion:

This Guideline should be implemented with due respect for Data Protection Laws and under a standard of reasonableness and good faith. Doing so will minimize any potential conflict arising between Company's U.S. eDiscovery and non-U.S.

data protection obligations.[51] If there is doubt as to what action would be appropriate, the Company DPO, In-House counsel, and the eDiscovery Team should be consulted.

51. *See* International Litigation Principles, *supra* note 36, Principles 1–2.

Frequently Asked Questions (FAQ)

Model Language to be customized by Company

This FAQ addresses issues that may arise when implementing the Guideline. The purpose of this FAQ is to provide awareness of the complexity of electronic data protection in a cross-border environment. The FAQ offers points to consider; it does not provide definitive answers, and may not apply to every situation. You should consult the eDiscovery Team before proceeding.

This FAQ will be updated from time to time as additional questions are asked. It has been designed to avoid duplication of the Group Data Protection Guideline and FAQ (available ***here***) as much as possible.

1. Introductory Questions

1.1 Who should read this FAQ?

The intended audience is those working in conjunction with the eDiscovery Team and whose role involves the transfer of non-U.S. data across international borders, typically for the purposes of U.S. litigation or other judicial proceedings.

1.2 Why is electronic data protection important?

Company is legally required to protect personal data and respect applicable privacy rights across all of its global operations. Data Protection Laws vary across jurisdictions; breach of the local laws can be met with financial penalties, regulatory sanctions, or criminal prosecutions. In addition, failure to process personal data according to established data protection principles could result in reputational damage to the brand and diminished consumer confidence.

1.3 Where can I find the Guideline?

It can be found on the Company's Intranet ***here***.

1.4 What is the role of the eDiscovery Team?

The eDiscovery Team assists in ensuring consistent compliance with Company's eDiscovery and data protection obligations. The eDiscovery Team does this in part by coordinating the involvement of appropriate subject matter experts. Depending on the situation, this may include Group Legal, Data Protection Officers, Outside counsel, and Company's Works Councils. Failure to consult the eDiscovery Team when processing non-U.S. personal data for legal proceedings in the U.S. could result in negative consequences for you and/or Company.

1.5 What are some basic principles of which I should be aware?

The Guideline incorporates, where appropriate, the International Litigation Principles.[52] Although the International Litigation Principles are advisory and do not carry the force of law, they provide guidance to public and private parties, counsel, data protection authorities, and the judiciary regarding the management of conflicts that may arise when there is an obligation in one jurisdiction to preserve or produce information from a second jurisdiction, and the laws of the second jurisdiction limit the preservation, processing, or transfer of such information.

You should familiarize yourself with the principles in the Guideline. They explain the importance of being aware of your obligations and working towards solutions that demonstrate

52. International Litigation Principles, *supra* note 36.

good faith, reasonableness, and 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. Key Questions

2.1 Does the Guideline prohibit the cross-border transfer of personal data?

No. There is no blanket prohibition on cross-border transfers of personal data. The Guideline recognizes that certain countries require that appropriate safeguards be implemented prior to the transfer of personal data. You should consult the eDiscovery Team before transferring any data across international borders.

2.2 What is Personal Data?

Personal data is any data containing information that (i) can be used to identify a Data Subject to whom such data relates, or (ii) is or might be directly or indirectly linked to an identifiable Data Subject. If there is any doubt as to whether data is personal, you should consult the local Company Data Protection Officer and the eDiscovery Team for guidance.

Some examples of personal data (non-exhaustive list) include the following: name, date of birth, gender, home address, home phone numbers, personal mobile phone numbers, an employee's CV information or talent profile, national identifiers, client identification numbers, and bank account or credit card numbers.

The Group Data Protection Guideline (available ***here***) provides additional information.

2.3 Does the use of personal data in legal proceedings supersede data protection obligations?

No, data protection safeguards must still be adhered to, although the need to submit personal data may be justified due to the fact that there is a legal proceeding. The eDiscovery Team and local Company Data Protection Officer should be consulted on specific matters.

2.4 What is the Email Archive?

The Email Archive is a storage system for some or all emails sent or received by Company email accounts for a [length of time] period. Additional information about the Archive can be found on the Company's Intranet ***here***.

2.5 What are "blocking statutes"?

Blocking statutes are laws designed to restrict the disclosure of personal data and other covered information to foreign jurisdictions. For example, a U.S. court may order the disclosure of personal data of a French employee with such data being located in France, creating a potential conflict of U.S. law (requiring the production) and French law (prohibiting the production). Similar restrictions exist in Switzerland. Accordingly, data transfers potentially subject to blocking statutes require a case-by-case assessment and you should consult the eDiscovery Team and local Company Data Protection Officer for guidance.

2.6 What is a Works Council or Workers' Council?

A Workers' Council (sometimes also referred to as a Works Council) is an organization representing employees at a local or firm level. Workers' councils have been established in, for example, Germany, France, and the Netherlands. You

should consult the eDiscovery Team prior to processing personal data of Company employees from the countries that have established such Councils.

2.7 What constitutes a cross-border "transfer" of personal data?

The cross-border "transfer" of personal data may include disclosure of personal data to a recipient employed or contractually bound by a third party in a different country, even if such recipient is within the same organization. Making this information accessible remotely is also considered a "transfer." Similarly, allowing the recipient to process the personal data by, among other things, collecting, recording, accessing, using, storing, altering, retrieving, or consulting (reading) the data constitutes a "transfer." If you have any doubts as to what may constitute a transfer, you should consult the eDiscovery Team.

2.8 In my case, Outside counsel conducts cross-border productions of personal electronic data. Should I still consult the eDiscovery Team?

Yes. While many outside law firms have good cross-border data transfer processes, ultimate responsibility remains with Company. Further, Outside counsel may not be sufficiently familiar with local data protection restrictions or have a comprehensive understanding of the physical location of information environments and data storage facilities of the Company. Accordingly, you should consult the eDiscovery Team to ensure compliance with internal policies and applicable laws and to maintain appropriate communication with internal stakeholders.

2.9 A European employee of Company consented for his or her personal electronic data to be used in a U.S. proceeding. Should I still consult the eDiscovery Team?

Yes. While employee consent is sufficient in many instances, there are still regulations regarding the nature and form of employee consent. For instance, in some European jurisdictions the validity of employee consent may be questioned on the basis that it may not have been given voluntarily. Also, Company may need to undertake additional steps in light of, for example, blocking statutes and the Swiss Penal Code.

2.10 A European employee wants to see the documents that are to be or have been produced by Company in a U.S. proceeding. Does he/she have such a right?

Potentially, European (and other) Data Protection Laws provide the Data Subject certain rights of access to their personal data processed by Company. However, there may be legal restrictions on allowing access to the personal data of other parties. If you are confronted with a Data Subject access request, you should consult local Company Data Protection Officers and the eDiscovery Team to ensure compliance with internal policies and applicable law and to maintain appropriate communication with internal stakeholders.

2.11 Does European employee personal data have to be redacted?

In the case of a civil litigation, employee and other personal data contained in business documents to be disclosed usually do not have to be redacted. There may be cases where redactions are required or appropriate (e.g., in certain investigations of potentially criminal conduct by foreign authorities). However, even if no redactions have to be made, internal

and sometimes external data protection safeguards should be considered with regard to business documents that contain personal data of persons from Europe or other countries with applicable Data Protection Laws. You should consult the eDiscovery Team on these issues and make sure that Outside counsel considers them early on in the process.

2.12 Are special arrangements required with Outside counsel?

In the event that Company retains non-European Outside counsel to handle personal data that is subject to European (or other) Data Protection Laws, special arrangements with Outside counsel will usually be necessary (e.g., including a data protection clause in the engagement letter or having Outside counsel sign the EU model clauses for cross border data transfers).

Outside counsel must be instructed properly on data protection issues and made aware of the restrictions (not only including data protection and privacy laws in the narrow sense, but also issues related to blocking statutes, business secrets, and labor laws, because violation of these restrictions may result in criminal liability). You should consult the eDiscovery Team on these issues.

Creating awareness with Outside counsel early on is important not only to ensure compliance with data protection and privacy laws, but also to ensure that counsel will represent Company adequately in dealing with opposing parties and authorities (e.g., in the meet-and-confer phase provided for by U.S. civil procedure law).

3. Country-Specific Questions

3.1 My U.S. legal proceeding involves only U.S. employees. Does this FAQ apply?

This FAQ addresses the cross-border transfer of non-U.S. data, not the use of U.S. data in U.S. legal proceedings. U.S. laws and regulations on data protection and data transfers differ significantly from Data Protection Laws and regulations in Europe, Asia, Latin & South America, and other regions.

Nevertheless, you should still consult the eDiscovery Team. There is no such thing as an "eDiscovery case;" every litigation and arbitration involves eDiscovery. The eDiscovery Team, as Company's subject matter experts, is here to assist and ensure consistent compliance with Company's eDiscovery obligations.

3.2 I'm transferring personal data out of Switzerland. What should I do?

Consult the eDiscovery Team. The eDiscovery Team will be able to assist you with the correct process to ensure that Company's obligations are met, as these will vary depending on the destination of the data you are transferring.

Switzerland is not within the EU, and although Swiss data protection law is comparable to the Data Protection Laws within the EU, there are differences (as there are certain differences also within the EU). For example, Switzerland has a different definition of what constitutes "personal data," as it also includes personal data about legal entities, not just individuals.

In addition, the Swiss Penal Code may be implicated depending on whether the disclosure of personal data is "forced" (in other words, performed upon the direct order of a non-Swiss governmental entity (e.g., a U.S. court, foreign regulator) with sanctions in case of non-compliance) or "unforced" (in other

words, performed voluntarily in furtherance of a legal obligation).[53] The Swiss Penal Code may also be implicated if business or manufacturing secrets of other Swiss third parties are at issue when Company knows that the business or manufacturing third party desires to keep the secret.[54]

3.3 I'm transferring personal data out of Germany. What should I do?

Consult the eDiscovery Team. The eDiscovery Team will be able to assist you with the correct process to ensure that Company's obligations are met, as these will vary depending on the destination of the data you are transferring.

Germany has enacted its own Data Protection Laws (based on the principles of the EU Directive). Germany has also established a Workers' Council, which, depending on the circumstances, may need to be consulted prior to the transfer of data. Furthermore, German law provides for detailed requirements with regard to contracts governing cases in which companies instruct third parties to process personal data on their behalf.

3.4 I'm transferring personal data out of France. What should I do?

Consult the eDiscovery Team. The eDiscovery Team will be able to assist you with the correct process to ensure that Company's obligations are met, as these will vary depending on the destination of the data you are transferring.

---

53. SCHWEIZERISCHES ZIVILGESETZBUCH [STGB], [SWISS PENAL CODE] Dec. 21, 1937, SR 311.0, art. 271.

54. SCHWEIZERISCHES ZIVILGESETZBUCH [STGB], [SWISS PENAL CODE] Dec. 21, 1937, SR 311.0, art. 273.

France has enacted its own Data Protection Laws (based on the principles of the EU Directive). France has also established a Workers' Council, which, depending on the circumstances, may need to be consulted prior to the transfer of data. Depending on the circumstances, French Outside counsel and regulatory bodies may need to be consulted prior to the transfer of electronic data.

3.5 I'm transferring personal data out of Italy. What should I do?

Consult the eDiscovery Team. The eDiscovery Team will be able to assist you with the correct process to ensure that Company's obligations are met, as these will vary depending on the destination of the data you are transferring. Italy has enacted its own data privacy laws (based on the principles of the EU Directive).

3.6 I'm transferring personal data out of the Netherlands. What should I do?

Consult the eDiscovery Team. The eDiscovery Team will be able to assist you with the correct process to ensure that Company's obligations are met, as these will vary depending on the destination of the data you are transferring.

The Netherlands has enacted its own data privacy laws (based on the principles of the EU Directive). The Netherlands has also established a Workers' Council, which, depending on the circumstances, may need to be consulted prior to the transfer of data.

3.7 I'm transferring personal data out of the United Kingdom. What should I do?

Consult the eDiscovery Team. The eDiscovery Team will be able to assist you with the correct process to ensure that Company's obligations are met, as these will vary depending on the destination of the data you are transferring.

The United Kingdom has enacted its own Data Protection Laws (based on the principles of the EU Directive). Transfer of personal data to any other country, even one with stricter data protection and privacy requirements, must be considered on a case-by-case basis.

APPENDIX B: TEMPLATE CROSS-BORDER DISCOVERY MANAGEMENT FORM FOR IN-HOUSE EDISCOVERY TEAMS

What it is: A checklist of common tasks, which tracks activities, roles, and responsibilities a company may consider when faced with a new U.S. matter that requires preservation and collection of data from offices outside of the U.S.[55]

Who it is for: Primarily In-House counsel; although, it may be shared with key stakeholders, such as Outside counsel and law department management.

Why it is important: Helps In-House counsel quickly triage a new matter as well as document a reasonable process and reduce risk of miscommunication.

How to use it: May be customized for the client and the matter; fill it out as each phase approaches; circulate it to key stakeholders to confirm understanding and buy-in.

---

55. The Template Cross-Border Discovery Management Form has been converted to grayscale and reformatted for purposes of printing in *The Sedona Conference Journal*. To view this Form in color and its orginal format, *see* The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, Appendix B, at B-2, THE SEDONA CONFERENCE (Sept. 2015 Public Comment Version), https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Practical%20In-House%20Approaches%20for%20Cross-Border%20Discovery%20and%20Data%20Protection.

Cross-Border Discovery Management Form [Matter Name & Number]	In-House Case Team	eDiscovery Team	In-House IT Support	Law Firm (merits counsel)	Law Firm (eDiscovery)	Vendor
Identify						
• Identify relevant cross-border data sources						
• Compile a list of custodians and locations						
• Conduct employee interviews to determine relevant data locations						
Research						
• Research applicable laws that apply to the data sources identified						
• Consult guidelines and company policies (e.g. Model Guidelines)						
• Confer with specialized privacy counsel						
Plan						
• Identify and prepare safeguards						
▪ Seek a stipulation or court-mandated protective order						
▪ Draft consent and consider whether it needs to be translated						
• Hold introductory meeting with critical stakeholders						
▪ Communicate a general plan and timeline for data collection						
▪ Discuss the company's policies for cross-border data collections as well as relevant experiences						
▪ Discuss alternate cost models to determine impact on budget						
▪ Assign roles for each major group						
Preserve						
• Prepare a preservation plan with a phased approach						
▪ Issue legal hold notices to U.S. custodians first						
▪ Prepare to issue legal hold notices to non-U.S. custodians along with appropriate safeguards, e.g. consent						
• Define the scope and narrowly tailor both the substantive and custodial scope of data to be preserved outside the U.S.						
▪ Define the relevant time period for the case						
• Scope privacy issues with opposing party or regulator where possible and document any agreement						
Collect						
• Plan for a targeted collection						
▪ Learn about the key stakeholders, key systems, and country customs ahead of time						
• Plan logistics in detail prior to collection efforts						
• Engage vendor support as early as possible for collection and processing as necessary						
▪ Conduct planning sessions with the vendor staff and local IT resources where the collection will take place						
• Set up transparency checkpoints in addition to consent						
▪ Prepare a frequently asked questions document to address employee concerns						
▪ Prepare a detailed collection script						
▪ Document efforts to keep employees informed						
▪ Provide employees with the opportunity to review data and confirm acceptance of transfer, as well as the opportunity to remove personal folders or emails from the collection process						
Process						
• Filter down the data to what is relevant and necessary						
• Learn about key business terms, names, and dates and develop a keyword search list with the goal of eliminating irrelevant information from the data set						
Review						
• Consider whether to perform the review of data in-country						
▪ Consult with local privacy counsel, outside eDiscovery counsel, and vendor to consider available review options						
• Draft document review guidelines for attorneys performing the review						
▪ Include protocols for tagging documents with protected data						
Produce						
• Consider various safeguards for production of protected data, such as producing in an anonymized or redacted format						
• Consider tiered document review, e.g., produce responsive data collected from U.S. custodians first and determine whether further production from non-U.S. custodians is necessary						
Close						
• Prepare an inventory of all locations of the data preserved, collected, or produced during the matter						
• Prepare to release legal holds and return or dispose of the data promptly upon termination of a matter						

(R) Responsible (A) Accountable (S) Supportive (C) Consulted (I) Informed

APPENDIX C: TALKING POINTS INFOGRAPHIC FOR INTERNAL BUSINESS CLIENTS AND EMPLOYEES

What it is: An infographic that provides a basic, visual education about the conflict of law that clients face when collecting data from countries with Data Protection Laws.[56]

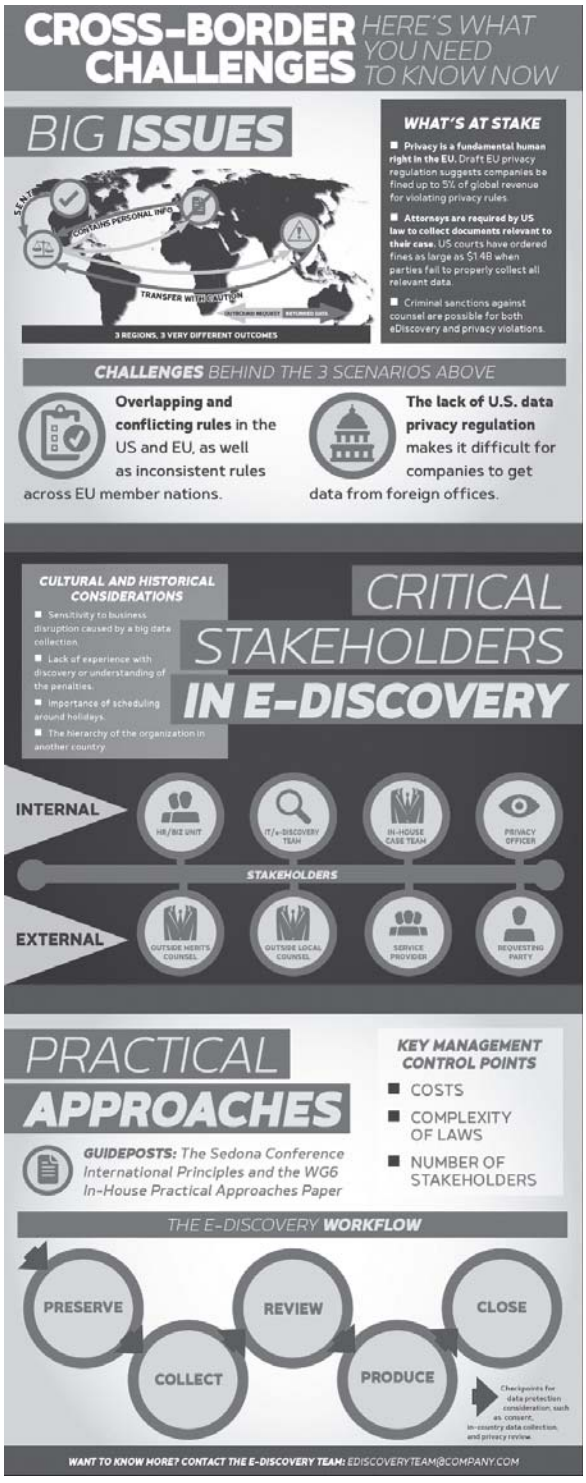
Who it is for: Internal business clients, employees, or legal counsel unfamiliar with the issues or company process.

Why it is important: Educates stakeholders why it is important to incorporate The International Litigation Principles into the matter handling process, demonstrates the complexity of managing the process as well as the need for appropriate resources, and previews what legal, cultural, and historical considerations may come into play.

How to use it: Can be used as a one-page infographic or as three separate panels for a PowerPoint presentation for stakeholders who may lack experience with the issues.

---

56. The Talking Points Infographic has been converted to grayscale for purposes of printing in *The Sedona Conference Journal*. To view this Infographic in color, *see* The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, Appendix C, at C-2, THE SEDONA CONFERENCE (Sept. 2015 Public Comment Version), https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Practical%20In-House%20Approaches%20for%20Cross-Border%20Discovery%20and%20Data%20Protection.


CROSS-BORDER CHALLENGES
HERE'S WHAT YOU NEED TO KNOW NOW
BIG ISSUES
SENT
CONTAINS PERSONAL INFO
TRANSFER WITH CAUTION
3 REGIONS, 3 VERY DIFFERENT OUTCOMES
WHAT'S AT STAKE
Privacy is a fundamental human right in the EU. Draft EU privacy regulation suggests companies be fined up to 5% of global revenue for violating privacy rules.
Attorneys are required by US law to collect documents relevant to their case. US courts have ordered fines as large as $1.4B when parties fail to properly collect all relevant data.
Criminal sanctions against counsel are possible for both eDiscovery and privacy violations.
CHALLENGES BEHIND THE 3 SCENARIOS ABOVE
Overlapping and conflicting rules in the US and EU, as well as inconsistent rules across EU member nations.
The lack of U.S. data privacy regulation makes it difficult for companies to get data from foreign offices.
CULTURAL AND HISTORICAL CONSIDERATIONS
Sensitivity to business disruption caused by a big data collection.
Lack of experience with discovery or understanding of the penalties.
Importance of scheduling around holidays.
The hierarchy of the organization in another country.
CRITICAL STAKEHOLDERS IN E-DISCOVERY
INTERNAL
HR/BIZ UNIT
IT/e-DISCOVERY TEAM
IN-HOUSE CASE TEAM
PRIVACY OFFICER
STAKEHOLDERS
EXTERNAL
OUTSIDE MERITS COUNSEL
OUTSIDE LOCAL COUNSEL
SERVICE PROVIDER
REQUESTING PARTY
PRACTICAL APPROACHES
GUIDEPOSTS: The Sedona Conference International Principles and the WG6 In-House Practical Approaches Paper
KEY MANAGEMENT CONTROL POINTS
COSTS
COMPLEXITY OF LAWS
NUMBER OF STAKEHOLDERS
THE E-DISCOVERY WORKFLOW
PRESERVE
COLLECT
REVIEW
PRODUCE
CLOSE
Checkpoints for data protection consideration, such as consent, in-country data collection, and privacy review.
WANT TO KNOW MORE? CONTACT THE E-DISCOVERY TEAM: EDISCOVERYTEAM@COMPANY.COM

APPENDIX D: EXEMPLAR HEAT MAP OF DATA PROTECTION AND DATA PRIVACY REGULATIONS

What it is: Example of a map that depicts an individual company's internal risk profile, color-coded by country.[57] A key feature of the map is an interactive "pop up" menu summarizing key Data Protection Laws, possible transfer mechanisms, key stakeholders, possible next steps, and applicable company policies or documents, like the Model Guideline (Appendix A).

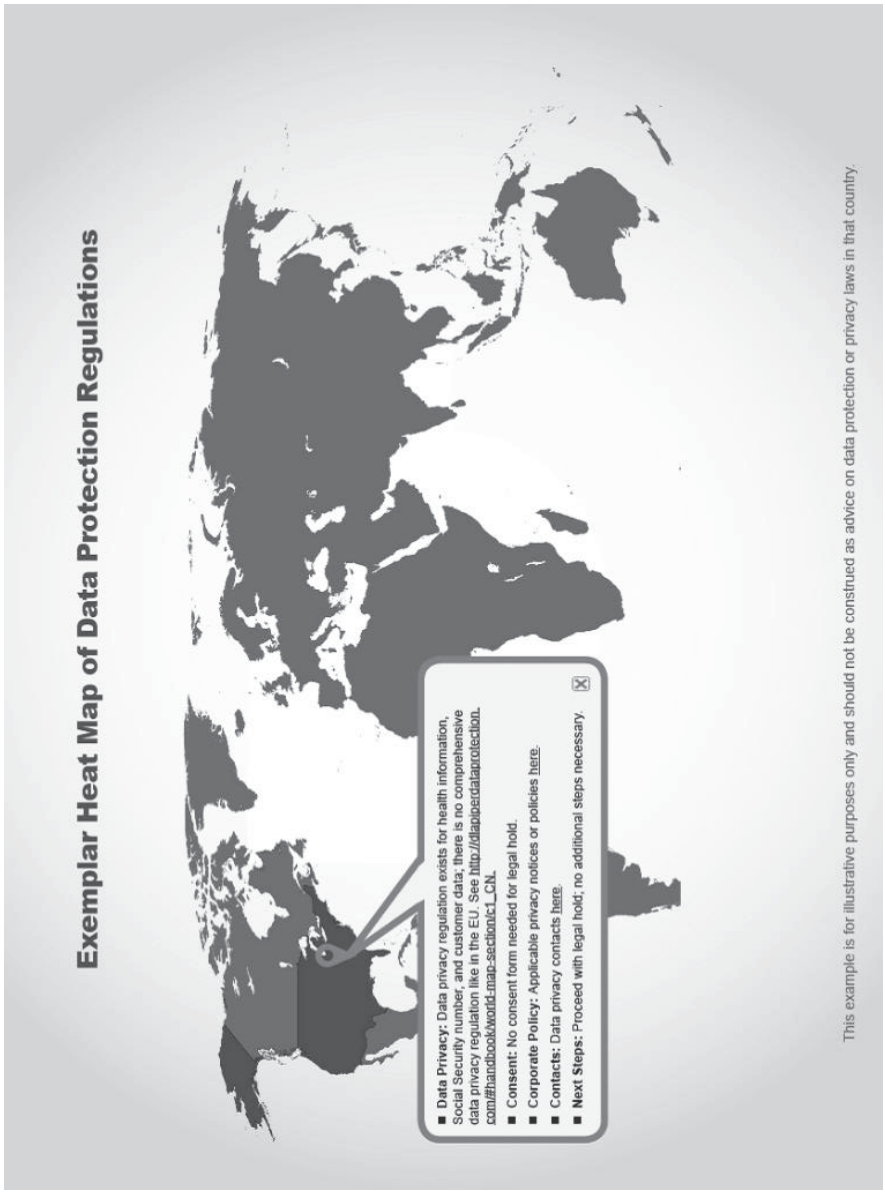
Who it is for: Primarily In-House legal and compliance departments.

Why it is important: Builds speed, efficiency, and consistency in In-House counsel who may need to juggle a number of jurisdictions and considerations for these types of matters.

How to use it: Although the example suggests providing certain data to the user, In-House counsel can customize their internal heat map in any way that helps tackle these types of matters.

---

57. The Exemplar Heat Map has been converted to grayscale for purposes of printing in *The Sedona Conference Journal*. To view this map in color, *see* The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, Appendix D, at D-2, THE SEDONA CONFERENCE (Sept. 2015 Public Comment Version), https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Practical%20In-House%20Approaches%20.


Exemplar Heat Map of Data Protection Regulations
Data Privacy: Data privacy regulation exists for health information, Social Security number, and customer data; there is no comprehensive data privacy regulation like in the EU. See http://dlapiperdataprotection.com/#handbook/world-map-section/c1_CN.
Consent: No consent form needed for legal hold.
Corporate Policy: Applicable privacy notices or policies here.
Contacts: Data privacy contacts here.
Next Steps: Proceed with legal hold; no additional steps necessary.
This example is for illustrative purposes only and should not be construed as advice on data protection or privacy laws in that country.