wgs

The Sedona Conference

Commentary on Managing International Legal Holds

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

August 2022
Public Comment Version
Submit comments by October 30, 2022,
to comments@sedonaconference.org

The Sedona Conference Commentary on Managing International Legal Holds

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

AUGUST 2022 PUBLIC COMMENT VERSION

Author: The Sedona Conference

Editor-in-Chief

Ronni Dawn Solomon

Contributing Editors

Franziska Fuchs
Eric P. Mandel
Kimberly A. Quan
Jennifer Tudor Wright
Brad Harris
Daryl Osuch, Sr.
John C. Tredennick

Steering Committee Liaison

Hon. James C. Francis IV (ret.)

Staff Editors

David Lumia
Michael Pomarico

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

Preface

Welcome to the public comment version of The Sedona Conference *Commentary on Managing International Legal Holds* ("*Commentary*"), a project of The Sedona Conference Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG6 is to develop principles, guidance and best practice recommendations for information governance, discovery and disclosure involving cross-border data transfers related to civil litigation, dispute resolution and internal and civil regulatory investigations.

The Sedona Conference acknowledges Editor-in-Chief Ronni Solomon for her leadership and commitment to the project. We also thank Contributing Editors Franziska Fuchs, Brad Harris, Eric Mandel, Daryl Osuch, Kimberly Quan, John Tredennick, and Jennifer Tudor Wright for their efforts, and Judge Jay Francis for his guidance and input as Steering Committee liaison to the drafting team.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG6 who reviewed, commented on, and proposed edits to early drafts of the *Commentary* that were circulated for feedback from the Working Group membership. Other members provided feedback at WG6 meetings where drafts of this *Commentary* were the subject of the dialogue. On behalf of The Sedona Conference, I thank all of them for their contributions.

Please note that this version of the *Commentary* is open for public comment, and suggestions for improvement are welcome. Please submit comments by October 30, 2022, to comments@sedonaconference.org. The editors will review the public comments and determine what edits are appropriate for the final version.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG6 and several other Working Groups in the areas of electronic document management and discovery, data security and privacy liability, international data transfers, patent litigation, patent remedies and damages, and trade secrets. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
August 2022

Table of Contents

PREAMBLE

Parties in actual or anticipated cross-border litigation face a conundrum. On one hand, they are often required to comply with strict requirements for the preservation of discoverable data. On the other, privacy laws and regulations can severely restrict their legal ability to preserve personal data.

Although issues arise whenever preservation obligations and privacy requirements conflict, *The Sedona Conference Commentary on Managing International Holds* ("*Commentary*") focuses primarily on preservation obligations in the United States, because the U.S. arguably has the most comprehensive and significant preservation requirements of any country. Correspondingly, in discussing international data protection laws, the paper focuses mostly on the European Union's General Data Protection Regulation (GDPR)[1] because it is highly influential and has spurred, and continues to spur, similar regulations in other jurisdictions around the world.

While this *Commentary* will allude to other preservation and privacy regimes, it will not explore them in depth. By analyzing the application of GDPR in the context of U.S. preservation obligations, it sets out to provide a framework for counsel when applying international legal holds in any jurisdiction with conflicting data protection laws. It is hoped that readers will find it useful as they analyze and take steps to meet legal hold and data protection obligations.

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents [hereinafter GDPR].

I. INTRODUCTION

In 2007, The Sedona Conference Working Group 1 ("Sedona WG1") published for public comment the First Edition of *The Sedona Conference Commentary on Legal Holds: The Trigger & the Process*.[2] Sedona WG1 released the final version in 2010,[3] which provided commentary and guidelines for the implementation and management of legal holds, with a primary focus on U.S. litigation and investigations.

In 2019, Sedona WG1 published *The Sedona Conference Commentary on Legal Holds, Second Edition: The Trigger & The Process*, which provided both an update on legal cases released after publication of the First Edition and commentary on the impact of the 2015 Amendments to the Federal Rules of Civil Procedure.[4] The Second Edition similarly focused on U.S. litigation and government investigations, but added Guideline 12, which addressed the implications of preserving information located outside the United States:

> Guideline 12: An organization should be mindful of local data protection laws and regulations when initiating a legal hold and planning a legal hold policy outside of the United States.[5]

The purpose of this *Commentary* is to expand on Guideline 12 by focusing on "international legal holds," defined as legal holds involving preservation obligations that cross international borders. The intent is to provide guidance and practice points for implementing international legal holds while at the same time complying with potentially conflicting international data protection laws and regulations (hereinafter "international data protection laws").

This *Commentary* does not focus on cross-border data transfers, which may become an important consideration when collecting data to preserve, or transferring data to another jurisdiction for analysis or review (e.g., outside of the European Union (EU), in the case of GDPR).[6]

The *Commentary* is written with several audiences in mind:

- U.S. companies and lawyers handling cross-border preservation issues in litigation or investigations;

---

2 The Sedona Conference, *Commentary on Legal Holds: The Trigger & The Process*, Public Comment Version (Aug. 2007), *available at* https://thesedonaconference.org/publication/Commentary_on_Legal_Holds.

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

4 The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341 (2019), available at https://thesedonaconference.org/publication/Commentary_on_Legal_Holds [hereinafter *Sedona Commentary on Legal Holds, Second Edition*].

5 *Id.* at 409.

6 GDPR articles 44 to 50 govern the transfer of data outside of the EU and require separate justification before the data can be transferred. *See also* The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, 17 SEDONA CONF. J. 397 (2016).

- Non-U.S. lawyers or other legal professionals seeking to comply with U.S. preservation obligations or other jurisdictions' preservation requirements and, at the same time, data protection requirements in their own or other countries;

- Judges addressing whether, how, and under what circumstances parties should be required to preserve information where conflicts with international data protection laws are unavoidable;[7]

- Government agencies and authorities seeking the preservation of information stored in other jurisdictions; and

- Data protection authorities so they might better understand an entity's good-faith efforts and attempts to achieve compliance.

[7] *See, e.g.*, The Sedona Conference, *Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders*, 21 SEDONA CONF. J. 393 (2020).

II. PRESERVATION AND INTERNATIONAL DATA PROTECTION REQUIREMENTS

A. Preservation Obligations: The Duty to Preserve

In 2003, U.S. District Court Judge Shira Scheindlin set the stage for a new era in United States litigation when she stated in *Zubulake v. UBS Warburg*:

> Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents.[8]

Judge Scheindlin's admonition sprang from the longstanding common-law duty for litigants to prevent spoliation—the loss or destruction of relevant materials that may later be used by another at trial.[9] It also flowed from the principle of broad pretrial disclosure in the U.S. first established in 1938 and continuing through the promulgation of the Federal Rules of Civil Procedure.[10]

In the years since *Zubulake IV*, many U.S. organizations have established procedures and practices to enable the preservation of information—whether hard-copy documents, electronically stored information, or other evidentiary materials that may be subject to a discovery obligation (hereinafter "discoverable information") through the implementation of a legal hold.[11] While the terms "litigation

---

8 Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 218 (S.D.N.Y. 2003).

9 The Sedona Conference Glossary defines spoliation as: "The destruction of records or properties, such as metadata, that may be relevant to ongoing or anticipated litigation, government investigation, or audit." *The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition,* 21 SEDONA CONF. J. 263, 373 (2020), *available at* https://thesedonaconference.org/publication/The_Sedona_Conference_Glossary. *See also* Robert Keeling, *Sometimes Old Rules Know Best: Returning to Common Law Conceptions of the Duty to Preserve in the Digital Information Age*, 67 CATH. U. L. REV. 67 (2018) (historical background of common law duty to preserve and comparing application of today's standard).

10 Fed. Judicial Ctr., *Federal Rules of Civil Procedure Establish Uniformity* (Sept. 16, 1938), https://www.fjc.gov/history/timeline/federal-rules-civil-procedure-establish-uniformity (last visited Aug. 18, 2022). Many states in the U.S. have adopted rules modeled on the Federal Rules of Civil Procedure and allow broad pretrial discovery. Conference of Chief Justices, Federal Rules of Civil Procedure, https://ccj.ncsc.org/news/frcp (last visited Aug. 18, 2022).

11 This *Commentary* uses the phrase "discoverable information" consistent with the *Sedona Commentary on Legal Holds, Second Edition*, *supra* note 4, at 348. The authors recognize that information deemed to be relevant may vary from case to case, especially in civil litigation, where some parties may take a narrower position, versus governmental investigations, where relevancy can be very broadly construed. The goal of this *Commentary* is to help practitioners and others navigate between even the most demanding legal hold obligations and privacy protections. The authors also note that the more demanding the preservation obligation, the stronger the argument is for meeting the necessity requirement imposed by the GDPR and similar rules. *See infra* Section II.C.2.a.

hold" and "legal hold" are often used interchangeably, this *Commentary* uses the broader term "legal hold" to encompass government investigations as well as civil litigation.[12]

Thus, U.S. organizations and others subject to U.S. civil litigation are required to preserve discoverable information when they "reasonably anticipate" litigation or an investigation.[13] To comply with U.S. preservation obligations, an organization will need to consider taking a number of steps. These may include (1) sending a written legal hold notice to individuals likely to be the custodians of discoverable information; (2) suspending routine deletion or destruction policies for discoverable information; (3) adopting "preservation in place" strategies to suppress manual alteration or deletion within systems that hold discoverable information; and (4) copying sources to a centralized location to ensure the information will be available during the discovery process. The legal framework and guidelines for compliance with U.S. preservation obligations are detailed in the *Sedona Commentary on Legal Holds, Second Edition*.[14]

Failing to meet U.S. preservation obligations may lead to sanctions, including curative measures and sanctions such as instructing the jury to presume that the information was unfavorable to the party that failed to meet its preservation obligation, monetary payments, or even dismissal of the action or the entry of a default judgment.[15] It also may include civil tort liability and criminal penalties for destruction of evidence.[16]

Non-U.S. Preservation Obligations: In non-U.S. jurisdictions, the extent of preservation obligations often turns on whether the jurisdiction follows common law or civil law and whether the matter relates to a private civil matter or a governmental investigation.[17] For example, common law countries such as the United Kingdom, Canada, Australia, and New Zealand recognize an obligation to preserve relevant documents in the context of civil litigation and investigations.[18] In the UK, a party is required to preserve and disclose all documents on which it relies as well as those that ad-

---

12 *See In re* Delta/Airtran Baggage Fee Antitrust Litig., 770 F. Supp. 2d 1299, 1307–08 (N.D. Ga. 2011) (recognizing that preservation obligations apply to government investigations).

13 *Zubulake IV,* 220 F.R.D. at 218.

14 *See Sedona Commentary on Legal Holds, Second Edition, supra* note 4.

15 *See* FED. R. CIV. P. 37(e).

16 18 U.S.C. § 1519.

17 *See* Kenneth N. Rashbaum, Matthew Knouff & Melinda C. Albert, *U.S. Legal Holds Across Borders: A Legal Conundrum?*, 13 N.C.J.L. & TECH. 69, 85 (2011), available at https://www.bartonesq.com/wp-content/uploads/2014/05/UNC-JOLT-Art_Rashbaum_Knouff_Albert_69_94.pdf. *See also* The Sedona Conference, *Framework For Analysis Of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery*, Public Comment Version (2008), at 14–16 [hereinafter *Sedona Framework*], *available at* https://thesedonaconference.org/publication/Framework_for_Analysis_of_Cross-Border_Discovery_Conflicts.

18 *See* James A. Sherer & Taylor M. Hoffman, *Cross-border Legal Holds: Challenges and Best Practices*, PRACTICAL LAW 28 (Oct./Nov. 2017), *available at* https://www.bakerlaw.com/webfiles/Litigation/2017/Articles/10-17-2017-Sherer-FeatureCrossBorder.pdf.

versely affect its case or support another party's case.[19] As set forth in UK Civil Procedure Rule Practice Direction 31B.7, "[a]s soon as litigation is contemplated, the parties' legal representatives must notify their clients of the need to preserve disclosable documents. The documents to be preserved include Electronic Documents which would otherwise be deleted in accordance with a document retention policy or otherwise deleted in the ordinary course of business."[20]

Civil law countries impose more limited preservation obligations. For example, German procedural rules, while not imposing a direct obligation to preserve, allow for the ease of evidentiary rules in cases where documents can no longer be produced.[21] France and Spain, similarly, have limited preservation obligations.[22]

In such jurisdictions, the absence of a duty to preserve evidence may create legal and cultural conflicts if the individual or legal entity is required to preserve evidence by another jurisdiction such as the U.S.[23]

B. International Privacy Requirements: The Rights of Individuals

A growing number of jurisdictions recognize that individuals have a fundamental right to privacy. Many have enacted data protection laws that protect the rights of natural persons by restricting the collection, use, storage, or alteration of their personal information.[24] In most cases, these laws restrict the transfer of personal information to jurisdictions that fail to provide adequate levels of protection.

---

19 UK CPR 31.6.

20 UK CPR Practice Direction 31B.7. *See How Relevant is Legal Hold to the UK Market?,* CYFOR, https://cyfor.co.uk/how-relevant-is-legal-hold-to-the-uk-market/ (last visited Aug. 18, 2022).

21 As a rule, the parties provide documents they will rely on to support their case in their trial briefs, including the opponent's documents. Where a requesting party relies on a producing party's document to support its brief, the requesting party can move the court for an order compelling the producing party to produce the document to the court. ZIVILPROZESSORDNUNG [ZPO] [CODE OF CIVIL PROCEDURE] art. 425. Where the producing party cannot or does not produce the document to the court, the court can either accept a copy of the document provided by the requesting party as sufficient or can accept the requesting party's characterization of the contents of the document as evidence. *Id.*, art. 427. The preservation of documents is therefore in the interest of the parties.

22 *See, e.g.,* Olivier de Courcel, *The e-Discovery and Information Governance Law Review: France,* THE LAW REVIEWS (May 4, 2021), https://thelawreviews.co.uk/title/the-e-discovery-and-information-governance-law-review/france; Enrique Rodríguez Celada, Sara Sanz Castillo & Reyes Bermejo Bosch, *The e-Discovery and Information Governance Law Review: Spain*, THE LAW REVIEWS (May 4, 2021), https://thelawreviews.co.uk/title/the-e-discovery-and-information-governance-law-review/spain.

23 *See Cross Border Investigations Update, Legal Holds in Cross-Border Investigations*, SKADDEN (Aug. 2018), https://www.skadden.com/insights/publications/2018/08/cross-border-investigations-update#legal.

24 GDPR, *supra* note 1, art. 1 (*Subject-matter and objectives*); *id.* at art. 4(1).

Personal Data: The GDPR is an influential and prominent example of a comprehensive data protection law[25] that protects the rights of individuals with respect to their personal information. The GDPR took effect on May 25, 2018, and is binding on all Member States of the European Union[26] as well as the Member States of the European Economic Area (EEA).[27] Under the GDPR, "'personal data' means any information relating to an identified or identifiable natural person ('data subject')."[28] It is broadly defined and includes anything that can be categorized as "individual information." For example, it includes information that shows the relationship of a person to his or her environment, objects or third parties, as well as his or her financial situation (assets, salary, creditworthiness), contractual relationships, friendships, ownership, consumption or communication behavior, working hours, email addresses, and so on.[29] It also includes the data subject's name, age, origin, gender, education, marital status, address, date of birth, eye color, fingerprints, genetic data, state of health, photographs and video recordings, personal beliefs, preferences, behaviors, or attitudes.[30] Likewise, personal information also applies to both content and metadata such as IP (internet protocol) addresses, cookies, or radio frequency identifiers.[31] Even where a subject's identity has been replaced by a pseudonym, the information is still considered personal information.[32]

The key point is that data subjects have protected rights under the GDPR regarding the use of their personal information—regardless of whether the personal data in question relates to their private life or is part of their employer's business documents.[33] Hereafter, the terms "personal information" and "personal data" are used interchangeably.[34]

---

25 The GDPR replaced the 1995 Data Protection Directive. The GDPR established the European Data Protection Board (EDPB), which contributes to the consistent application of data protection rules throughout the EU. *See* European Data Protection Board, *Who we are*, https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en. The EDPB's predecessor was the Article 29 Working Party. The work of the Article 29 Working Party resulted in the development of the GDPR.

26 *See* GDPR, *supra* note 1, art. 99 (*Entry into force and application*), *id.* at Art. 3 (*Territorial scope*).

27 Specifically, Iceland, Norway and Liechtenstein.

28 *Id.*

29 Case C-342/12, Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT), 2013 European Court of Justice, https://curia.europa.eu/juris/document/document.jsf?text=&docid=137824&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1. *See also* BORIS PAAL & DANIEL A. PAULY, DATENSCHUTZ-GRUNDVERORDNUNG BUNDESDATENSCHUTZGESETZ: DS-GVO BDSG, 3. Auf. (2021), Art. 4, Rn. 14.

30 *Id.*

31 *Id.*, Art. 4, Rn. 18.

32 GDPR, *supra* note 1, Recital 26, https://gdpr-info.eu/recitals/no-26/.

33 SPIROS SIMITIS, ET AL., DATENSCHUTZRECHT, 1. Auf. (2019), Art. 88, Rn. 1.

34 The reader should be mindful, however, of personal information that, because of its sensitivity, requires a higher degree of protection. Unless the context otherwise makes it clear, that information is not the subject of the paper.

Processing: Under the GDPR, organizations must process personal information lawfully, fairly, and in a transparent manner as it relates to the data subject.[35] "Processing" is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use . . . ."[36] It also includes holding onto personal information after it should have been deleted.[37] Most relevantly to this *Commentary*, it includes the preservation of documents in connection with a legal hold.[38]

Controllers and Processors: To protect data subjects' rights, the GDPR focuses on "controllers" and "processors." Controllers are organizations or individuals that make decisions over the how and why of the processing of personal data.[39] Processors are organizations or individuals that process information on behalf of, and under the instructions of, controllers.[40]

A controller would include a company processing personal data on its internal information technology (IT) systems for purposes of its business. A processor could be any IT service provider to whom the company has outsourced processing tasks, such as a hosting provider, a records management company, a customer hotline, or an employee benefits company.

Extraterritorial Jurisdiction: The GDPR asserts extraterritorial jurisdiction. It applies to controllers and processors who are established or doing business in the EU regardless of whether they process any personal information in the EU or elsewhere.[41] It also applies to controllers and processors located outside the EU if they offer goods or services to people who are "in" the EU or who are monitoring the behavior of persons in the EU.[42]

---

35 GDPR, *supra* note 1, art. 5(1)(a).

36 *Id.*, art. 4(2).

37 *See, e.g., id. a*rt. 17 (i.e., right to be forgotten).

38 *See, e.g., id.*, art. 4(2); this was also true prior to the adoption of the GDPR. *See* Working Document 1/2009 on pretrial discovery for cross border civil litigation, adopted on Feb. 11, 2009, 00339/09/EN WP 158, *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf. (Under Directive 95/46, any retention, preservation, or archiving of data for such purposes would amount to processing.).

39 *See e.g.,* GDPR, *supra* note 1, art. 4(7), which defines a controller as a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal information."

40 *See id.*, art. 4(8), which defines a processor as a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." A "controller" can also be a "processor."

41 *See id.*, art. 3(1).

42 *Id.* at art. 3(2) and 3(3). Recital 25 clarifies that Article 3(3) refers to those places which, according to international law, are not subject to the third country in which they are geographically located. These are in particular the diplomatic or consular representations of a Member State in a foreign country outside the European Union. This third scenario is unlikely to occur in the legal hold context and is therefore not discussed further.

Penalties and Sanctions for Violations: Failing to comply with the GDPR's requirements may expose a controller or processor[43] to severe monetary penalties—up to 20 million Euros or 4 percent of the violator's worldwide annual gross revenue for the prior year, whichever is higher.[44] Violators may also be subject to nonmonetary administrative sanctions and may be required to pay compensation to data subjects whose rights have been violated.

C. Preservation Under the GDPR

Two GDPR provisions govern the implementation of preservation steps. First, preservation must comply with Article 5, which sets out a series of guiding principles that govern all processing of personal information.[45] Second, preservation must comply with Article 6, which sets out requirements that must be followed to make processing lawful.[46] A party must satisfy both provisions in order to preserve information lawfully.[47]

1. Meeting Article Five's Guiding Principles

Article 5, Paragraph 1 sets forth "Principles relating to the processing of personal data," stating that personal information shall be:

a. Processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ("purpose limitation");

c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");

d. Accurate and, where necessary, kept up to date ("accuracy");

e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information are processed; ("storage limitation"); and

---

43 *See id.*, art. 4(8).

44 *Id.*, art. 83(5).

45 *Id.* at art. 5(1)(a-f).

46 *Id.* at arts. 7–8, 9–11, and 12–23.

47 European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, at 3 (adopted 25 May 25, 2018), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

f. Processed in a manner that ensures appropriate security of the personal information, ("integrity and confidentiality").

The controller is further responsible to demonstrate compliance with these principles when processing such data ("accountability").[48]

Although described as "principles," these provisions are in fact binding regulations applicable to controllers and processors and apply to every aspect of processing, including the preservation of personal information and implementation of legal holds.[49] Most importantly, they shape and inform all other provisions of the GDPR.[50] A violation of these principles makes the data processing unlawful and exposes the wrongdoer to potentially severe sanctions.[51]

Although each must be considered carefully, several of the principles are particularly important in the context of implementing preservation steps for a U.S. legal hold:

Lawfulness: Data processing is permitted under certain conditions set out in the GDPR. The permissible conditions are based on weighing the data subject's fundamental human right to data protection against the lawful, legitimate purpose, interest, and obligations of the controller.[52] Establishing a lawful basis under Article 6, explained in more detail below, is a prerequisite for processing in the context of a legal hold.

Transparency: The principle of transparency is an essential principle related to the processing of information. It does not merely imply a right for the data subject to request information.[53] It also includes the obligation of the controller to actively provide the data subject with all information necessary to enable the data subject to verify whether processing is lawful and to exercise his or her rights.[54] Without sufficient transparency, the data subject is effectively deprived of his or her fundamental human rights.[55] Therefore, where a controller collects personal information from a data subject, it is obliged, even without a data subject requesting it, to inform the subject that data is being

---

48 *See* GDPR, *supra* note 1, art. 5(1)(a-f) (paraphrased in part).

49 PAAL & PAULY, *supra* note 30, Art. 5, Rn. 1.

50 Alexander Roßnagel, in: SIMITIS, ET AL., *supra* note 33, Art. 5 Rz. 15.

51 GDPR, *supra* note 1, art. 83(5)(a).

52 *See* Charter of Fundamental Rights of the European Union, Art. 8, 2012 O.J. (C 326) 391 (26 Oct. 2012), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN (establishing the fundamental rights of the data subject); *See also,* GDPR, *supra* note 1, art. 5 (principles relating to the processing of personal data).

53 *Id.*, art. 12.

54 *Id.,* Recital 39 (Principles of Data Processing); Roßnagel, in: SIMITIS ET AL., *supra* note 33, Art. 5, Rz. 50.

55 *Id.*

collected and the purpose and effect of the collection.[56] The principle of transparency also requires that information and communication relating to the processing of personal information be easily accessible and easy to understand, and that clear and plain language be used.[57]

Purpose Limitation: Information may only be processed for specific, explicit, and legitimate purposes.[58] It may not be processed for abstract or general purposes nor retained for its potential future value and use to the controller. Processing for unspecified purposes is specifically prohibited.[59] A legitimate purpose must be identified when or before processing occurs. When there is no longer a legitimate purpose for such processing, the personal information must be deleted.[60]

Minimization: Data minimization describes a means-ends relationship: information may only be processed to the extent necessary to achieve the defined purpose for data processing.[61] This requirement limits the extent and depth of processing and thus minimizes the impact on the data subject's right to data protection. This principle also requires that the purpose be specified and pursued in a way that ensures as little personal information as possible is processed.[62] Additionally, the period for which personal data is stored is limited to the strict minimum.[63]

The principle does not call for a minimization of information per se. Rather, it is designed to reduce the potential harm and impact on a data subject's rights by reducing the amount of personal information processed or disclosed to what is unavoidably necessary.

Accountability: Under the accountability principle, the controller is responsible for, and must be able to demonstrate compliance with, Article 5.[64] The controller must actively take measures to implement the principles in its data processing operations. The controller must also document its actions and be able to prove compliance with the obligation.

---

56 *See* GDPR, *supra* note 1, Recital 39.

57 *Id.*

58 *Id.*, art. 5(1)(b); Roßnagel, in: SIMITIS ET AL., *supra* note 33, Art. 5, Rz. 69.

59 *Id.* at Rz. 72.

60 *See* GDPR, *supra* note 1, art. 17 (*Right to erasure ('right to be forgotten')*).

61 *Id.*, art. 5(1)(c); Bernard Marr, *Why Data Minimization Is An Important Concept In The Age of Big Data*, FORBES (Mar. 16, 2016), https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/?sh=3ceb8bc41da4 (last visited on Aug. 18, 2022).

62 Roßnagel, in: SIMITIS ET AL., *supra* note 33, Art. 5, Rz. 123.

63 GDPR, *supra* note 1, Recital 39.

64 *See* European Data Protection Supervisor, *Accountability,* https://edps.europa.eu/data-protection/our-work/subjects/accountability_en (last visited Aug. 18, 2022).

2. Establishing a Lawful Basis under Article Six

Article 6 begins with the unambiguous and fundamental statement: ***"****Processing shall be lawful only if and to the extent that one of the following applies.****"*** It then proceeds to enumerate six bases for lawful processing. The following are the most commonly considered in conjunction with preservation: (a) the legitimate interests of the controller or a third party, (b) consent of the data subject, and (c) compliance with a legal obligation.

(a) Pursuing a Legitimate Interest: The most common avenue for establishing a lawful basis for preserving personal information is pursuing a legitimate interest of the controller. The relevant GDPR provision provides:

> processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[65]

This provision requires the controller to show: (1) the controller's legitimate interest, (2) that the processing (preservation) is necessary to protect that interest, and (3) that the interest is not outweighed by the fundamental rights and freedoms of the data subject.

The threshold for showing what constitutes a controller's legitimate interest depends on the circumstances.[66] For example, defending or asserting a U.S. legal claim may be able to meet that threshold.[67] The mere possibility, however, of a U.S. legal proceeding, as opposed to reasonable anticipation of one, is not alone sufficient.[68]

The second factor that a controller must show—necessity—limits the extent of the processing to the defined purpose (e.g., defense of a legal claim). Processing may be deemed necessary if no less intrusive, but equally effective, means is available.[69]

---

65 GDPR, *supra* note 1, art. 6(1)(f).

66 Working Doc. 1/2009, *supra* note 38.

67 *Id.* at 2.

68 *Id.* at 8, 13 ("There may however be a further difficulty where the information is required for additional pending litigation or where future litigation is reasonably foreseeable. The mere or unsubstantiated possibility that an action may be brought before the U.S. courts is not sufficient.") ("However, the Working Party reiterates its earlier opinion that Art. 26 (1)(d) of the Directive cannot be used to justify the transfer of all employee files to a group's parent company on the grounds of the possibility that legal proceedings may be brought one day in U.S. courts.").

69 Schaffland/Holthaus, in: HANS-JÜRGEN SCHAFFLAND & NOEME WILTFANT, DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)/BUNDESDATENSCHUTZGESETZ (BDSG), Art. 6, Rn. 117c.

The third factor requires that once a legitimate interest and the requisite necessity have been established, the controller must show that its preservation requirements are not overridden by the interests of the data subject. As the Article 29 Working Party stated:

> Against these aims have to be weighed the rights and freedoms of the data subject who has no direct involvement in the litigation process and whose involvement is by virtue of the fact that his personal data is held by one of the litigating parties and is deemed relevant to the issues in hand, e.g. employees and customers.[70]

Thus, the controller must demonstrate that preservation is not outweighed by the interests of the data subject.[71] Issues to be considered include:

- The relevance of the preserved information to the matter;
- The consequences of preservation to the data subject; and
- The proportionality of the preservation efforts.

Ultimately, as the Article 29 Working Party stated: "The personal data must be adequate[,] relevant and not excessive in relation to the purposes for which they are collected and/or further processed."[72]

(b) Consent: Under Article 6(1)(a), a data subject may consent to the processing (in this case, preservation) of his or her personal information for one or more specific purposes.[73] Recital 32[74] and Article 7[75] set forth conditions for consent[76] and require that it be:

- in writing;
- explicit and freely given (without pressure or influence);
- unambiguous;

---

70 Working Doc. 1/2009, *supra* note 38, at 9; *See also* Art. 29 Working Party Working Document on surveillance of electronic communications for intelligence and national security purposes (WP228), at 9 (adopted Dec. 5, 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf.

71 Working Doc. 1/2009, *supra* note 38, at 9–10.

72 *Id.* at 10.

73 GDPR, *supra* note 1, art. 6(1)(a).

74 *Id.*, Recital 32.

75 *Id.*, art. 7.

76 *See also* Guidelines 2/2018, *supra* note 47, at 6–8.

- fully informed and include the right to withdraw; and
- given specifically for each specific matter requiring preservation.[77]

In addition, the controller must provide the individual with information about why the data is being collected or preserved, the specific legal basis the controller is relying on for preservation, and how to contact a data protection officer to lodge an objection.[78] Ultimately, the controller has the burden to demonstrate that these elements have been established.[79]

There are several risks to relying on consent as a lawful basis for preservation under the GDPR. First, data protection agencies and courts are reluctant to find that an employee can freely give consent to his or her employer because of the power imbalance inherent between employers and employees.[80] Valid consent between an employee and employer can be difficult to establish.[81]

Second, under the GDPR, a data subject can revoke his or her previously given consent at any time.[82] While revocation of consent does not make previous preservation activities unlawful, it might limit preservation options for the same information in the future. Future preservation could violate the GDPR even if an alternative lawful basis were otherwise available.[83]

---

77 A data subject must be informed in accordance with GDPR Article 13 information, which is to be provided where personal information is collected from the data subject.

78 GDPR, *supra* note 1, art. 13(1)(b-c).

79 *Id.*, Recital 42; Art. 7(1).

80 Winfried Veil, *Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis*, 71 NEUE JURISTISCHE WOCHENSCHRIFT, No. 46, 3337 (2018).

81 *See* SIMITIS, ET AL., *supra* note 33, Art. 88, Rn. 12. Because of this structural imbalance, employees are typically not in a position to achieve adequate protection of their personal data in the employment relationship by means of private autonomy. A particularly clear example of this is the consent of employees to the processing of their data by the employer, the voluntariness of which is often likely to be lacking if it is only given in the interests of the employer. Consequently, the national German data privacy law restricts the permissibility of employees giving their consent to the processing of their data in Section 26 (2) BDSG: "If the processing of personal data of employees is based on consent, the assessment of the voluntariness of the consent shall take into account in particular the dependency of the employee in the employment relationship and the circumstances under which the consent was given. Voluntariness may exist in particular if a legal or economic advantage is achieved for the employed person or the employer and the employed person pursue similar interests. Consent must be given in writing or electronically, unless another form is appropriate due to special circumstances."

82 GDPR, *supra* note 1, art. 7(3); *see* GDPR Recital 43.

83 Consent cannot easily be replaced with an alternative basis at a later time. "Even if a different basis could have applied from the start, retrospectively switching lawful basis is likely to be inherently unfair to the individual and lead to breaches of accountability and transparency requirements." UK INFORMATION COMMISSIONERS OFFICE, GUIDE TO THE GENERAL DATA PROTECTION REGULATION (GDPR) [hereinafter UK GUIDE TO GDPR], *Lawful basis for processing*, at 53 (Jan. 1, 2021), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ (last visited Aug. 19, 2022).

Third, obtaining consent simply may not be feasible. Certain documents may contain personally identifiable information of a number of individuals (e.g., an email conversation between several persons) and would require consent from all of them. While obtaining consent within a single organization may be an option, obtaining consent of data subjects such as former employees, customers, or suppliers will likely be difficult.

(c) Compliance with a Legal Obligation: Implementing preservation steps to comply with a legal obligation would seem to be another possible lawful basis under Article 6.[84] The phrase "legal obligation" under the GDPR, however, is expressly limited to an obligation that arises out of EU law or the law of an EU Member State.[85] As a result, this basis is largely inapplicable when preservation obligations arise pursuant to the laws of a non-EU jurisdiction.[86]

D. Jurisdictions Adopting Data Protection Regimes Similar to GDPR with Preservation Restrictions

Other nations have followed the EU's approach and adopted similar data protection laws. Below are examples of these laws, highlighting similarities and potential differences with the GDPR. These examples specifically focus on whether implementing preservation steps under a U.S. legal hold would potentially violate various data protection laws.

1. Europe: Non-EU Nations

United Kingdom: After leaving the EU, the UK enacted its own data protection law, which is substantively similar to the GDPR ("the UK GDPR").[87] Like the GDPR, the UK GDPR's definition of "processing" includes any set of operations performed on data, including the mere storage, preservation, hosting, consultation, or deletion of the data.[88] Accordingly, it is likely that implementing a U.S. legal hold involving personal information collected from natural persons who are located in the UK would be considered data processing under the UK GDPR and require the controller to comply

---

84 *See* GDPR, *supra* note 1, art. 6(1)(c).

85 *Id.* at Arts. 6(3) and 6(1)(f).

86 There may be instances where international treaties exist, such as the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (Hague Evidence Convention), that apply in a specific matter. In cases where a requesting party successfully serves the opposing party under the Hague Evidence Convention, that party may then be subject to preservation rules imposed on it by its own jurisdiction. However, some signatory states, such as Germany, have objected in part or fully to application to pretrial discovery through an objection according to Article 23, thus making it inapplicable in the context of a legal hold.

87 For a redline of the changes from EU GDPR to UK GDPR, see the General Data Protection Regulation Keeling Schedule, *available at* https://uk-gdpr.org/wp-content/uploads/2022/01/20201102_-_GDPR_-_MASTER_Keeling_Schedule_with_changes_highlighted_V3.pdf.

88 DLA Piper, *Collection and Processing: United Kingdom,* DATA PROTECTION LAWS OF THE WORLD, https://www.dlapiperdataprotection.com/index.html?t=collection-and-processing&c=GB (last modified 27 Jan. 27, 2021).

with that law.[89] The UK 2018 Data Protection Act, which enables the application of the EU GDPR in the UK, continues to supplement the UK GDPR.[90]

Switzerland: Switzerland is not an EU Member State but has its own data protection law called the Swiss Federal Act on Data Protection ("FADP"). It provides similar rights to those afforded by the GDPR.[91] The FADP defines processing as "any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data."[92] This is similar to the GDPR definition of processing,[93] and it is therefore likely that implementing a U.S. legal hold involving the personal information collected from individuals in Switzerland would be considered processing under the FADP and thus require the controller to meet the requirements of the FADP. The Swiss FADP's primary provisions are similar to the GDPR with only minor conceptual differences.[94]

2. Latin America

Brazil: Brazil's General Data Protection Law, Law 13.709 of 2018 (*Lei Geral de Proteção de Dados Pessoais*, or the "LGPD"), came into effect in 2020, with penalty provisions enforced beginning in 2021. The LGPD defines processing as any operation carried out with personal information, such as collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of the information, modification, communication, transfer, dissemination, or extraction.[95] This is similar to the GDPR's definition of processing.[96]

---

89 UK GDPR is nearly identical to GDPR and is explicitly extraterritorial in application. GDPR ADVISOR, https://uk-gdpr.org/territorial-scope. For example, in Article 3, the only difference is that the phrase "union" swapped for "United Kingdom." Thus, if a legal hold on a natural person in an EU country would constitute data processing under GDPR, then a legal hold on a natural person in the UK would also constitute data processing under the UK GDPR.

90 DLA Piper, *Law: United Kingdom,* DATA PROTECTION LAWS OF THE WORLD, https://www.dlapiperdataprotection.com/index.html?t=law&c=GB (last modified Jan. 27, 2021).

91 Federal Act of 19 June 1992 on Data Protection (FADP), SR 235.1; Ordinance of 14 June 1993 to the Federal Act on Data Protection (OFADP), SR 235.11; Ordinance of 28 Sept. 2007 on Data Protection Certification (DCPO), SR 235.13. For English translations, see Federal Data Protection and Information Commissioner (FDPIC), Legal Framework: Data Protection, *available at* https://www.edoeb.admin.ch/edoeb/en/home/the-fdpic/legal-framework.html. A new update to the FADP was approved in September 2020 and is expected to come into effect in 2022.

92 Federal Act on Data Protection (FADP), art. 3(e), unofficial English translation available at https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/en.

93 *See* GDPR, *supra* note 1, art.4(2).

94 A revised FADP will go into effect in 2022. *See Data Protected - Switzerland*, LINKLATERS, (last updated June 2022), https://www.linklaters.com/en/insights/data-protected/data-protected—-switzerland.

95 Lei No. 13.709, de 14 de Agosto de 2018, LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD), art. 5 X, *available at* http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

96 *See* GDPR, *supra* note 1, art.4(2).

Based on these similarities, it is likely that implementing a U.S. legal hold involving the personal information of Brazilian residents would be considered processing under the LGPD, thus requiring a controller to meet the requirements of the LGPD. Also similar to GDPR, there appear to be risks to relying on consent in Brazil as a lawful basis for preservation under the LGPD.[97]

Argentina: The Argentine Personal Data Protection Law, Act No. 25.326 of 2000 (the "PDPL"), does not define processing, but Section 2 of the Act defines a "data treatment" as any systematic operation or procedure, either electronic or otherwise, which enables the collection, integration, sorting, storage, change, relation, assessment, blocking, destruction, disclosure of data, or transfer to third parties.[98] This is similar to the GDPR's definition of processing.[99] The PDPL has been deemed adequate by the European Commission.[100] Based on these similarities and the adequacy determination, it is likely that implementing a U.S. legal hold involving the personal information of Argentine residents would be considered processing under the PDPL, thus requiring a controller to meet the requirements of the PDPL.

Uruguay: Data protection in Uruguay is governed by the Data Protection Act, Law No. 18.331 of 2008 and Decree No. 414/009 of 2009.[101] In 2012, the European Commission issued an adequacy determination allowing for open information transfers between the EU and Uruguay.[102] Given the adequacy determination and the fact that Uruguay's Data Protection Act is similar to the GDPR (although enacted a decade earlier), it is likely that implementing a U.S. legal hold involving the personal information of Uruguay residents would be considered processing, thus requiring a controller to meet the requirements of Uruguay's Data Protection Act.

---

97 Renato Leite Monteiro, *GDPR matchup: Brazil's General Data Protection Law*, IAPP (Oct. 4, 2018), https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/, (last visited on Aug. 19, 2022).

98 Personal Data Protection Act (PDPL) § 2 *(Definitions*), http://www.jus.gob.ar/media/3201023/personal_data_protection_act25326.pdf. *See* Florencia Rosati, *Argentina - Data Protection Overview*, ONETRUST DATA GUIDANCE, https://www.dataguidance.com/notes/argentina-data-protection-overview.

99 *See* GDPR, *supra* note 1, art.4(2).

100 *See* DLA Piper, *Law: Argentina,* DATA PROTECTION LAWS OF THE WORLD, https://www.dlapiperdataprotection.com/index.html?t=law&c=AR&c2=FR (last modified Jan 28, 2021).

101 Ley De Proteccion De Datos Personales, Ley No. 18331 (Aug. 11, 2008), *available at* https://www.impo.com.uy/bases/leyes/18331-2008. Reglamentacion de La Ley 18.331, Decreto No. 414/009 (Aug. 31, 2009), *available at* https://www.impo.com.uy/bases/decretos/414-2009.

102 Commission Implementing Decision of 21 Aug. 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data (2012/484/EU), 2012 O.J. (L 227) 11, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012D0484.

3. Asia-Pacific

Japan: Japan was one of the first Asian countries to pass a data protection law.[103] Its Act on the Protection of Personal Information ("APPI"), which took effect in 2017, is so similar to the GDPR in terms of fairness, purpose limitation, accuracy, storage limitation, integrity, confidentiality, and accountability that in July 2018, less than two months after the GDPR went into effect, the EU and Japan agreed to declare each other's data protection regimes adequate.[104] The APPI does not expressly define "processing," but given the overall similarities between the GDPR and the APPI, it is likely that implementing preservation steps as to personal information in compliance with U.S. law would be considered processing under the APPI.[105]

China: China has various laws that limit the collection and use of personal information, such as the Cyber Security Law of the People's Republic of China, which limits the collection and use of personal information (defined as information that alone or in combination with other information could be used to identify a person), establishes information security and data localization requirements, and provides for fines of up to RMB 1 million (roughly $150,000) for violations.[106]

China's Personal Information Security Specification ("PI Specification"), which took effect on October 1, 2020, also regulates the collection and use of personal information. It expands the definition of personal information to include information reflecting an individual's activities such as location data and online browsing history, and it adds the concept of Sensitive Personal Information, which includes a person's ID card number, bank account number, and the personal information of minors.[107] While there are various similarities between the current laws and the GDPR, it is not clear whether implementing preservation steps as to personal information in compliance with U.S. law would be considered processing.

---

[103] *See* Act on the Protection of Personal Information Law No. 57 of 2003, *unofficial translation available at* https://www.japaneselawtranslation.go.jp/en/laws/view/2781. Also, in 2016, the government agency now known as the Personal Information Protection Commission ("PPC"), was established.

[104] A tentative translation of Japan's Amended Act of Protection of Personal Information (APPI, version 2, Dec 2016) is available at https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf. The EU and Japan's "reciprocal adequacy" established the largest area of safe data flow in the world.

[105] The current version of the APPI distinguishes between public and private entities and applies to "business operators." However, recent revisions in April 2022 have brought other relevant laws in line with some APPI definitions: notably the definition of personally identifiable information (PII), and applications to public entities such that hospitals, other medical research institutions, and some public organizations that regularly use PII will fall under the APPI.

[106] *See* Rogier Creemers, et al., *Translation: Cybersecurity Law of the People's Republic of China [Effective June 1, 2017]*, NEW AMERICA (June 29, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

[107] National Standard of the People's Republic of China, Information security technology—Personal Information (PI) security specification, GB/T 35273-2020 (implementation date Oct. 1, 2020), English translation available at https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf. SPI is defined at § 3.2.

China is considering revisions to its data protection laws. On October 21, 2020, the first version of the draft Personal Information Protection Law ("Draft PIPL") was introduced. It would serve as China's first comprehensive data protection law and is intended to have a similar effect as the EU GDPR. It may go beyond the PI Specification. A second version of the Draft PIPL was issued on April 29, 2021.[108]

The Draft PIPL defines "personal information handling" to include the collection, storage, use, processing, transmission, provision, and publishing of personal information.[109] Further, the Draft PIPL more closely mirrors the GDPR, including, for example, its consent principles.[110] Given the similarities to the GDPR, it is likely that implementing a U.S. legal hold involving the personal information of Chinese residents would be considered processing under the Draft PIPL, but this draft has not yet been finalized and promulgated.[111]

Singapore: Singapore's Personal Data Protection Act ("PDPA") has a broad definition of processing similar to the GDPR that includes "recording" or "holding" data.[112] It is therefore likely that implementing preservation steps in compliance with United States law would be considered processing in Singapore and regulated by the PDPA.[113]

The PDPA has several differences from the GDPR. Consent under the PDPA is treated more broadly than under the GDPR and includes a number of exceptions allowing implied or "deemed" consent.[114] Similarly, there is no explicit requirement for data minimization. The purpose requirement for processing information also only requires a showing of reasonability.[115] Lastly, there is no extra level of protection for sensitive personal information such as race, ethnicity, or religion.[116]

---

[108] *See* Hunton Andrews Kurth, *China Issues Second Version of the Draft Personal Information Protection Law for Public Comments*, NAT'L L. REV. (May 4, 2021), *available at* https://www.natlawreview.com/article/china-issues-second-version-draft-personal-information-protection-law-public.

[109] Creemers, et al., *supra* note 106.

[110] Ken Dai & Jet Deng, *China's GDPR is Coming: Are You Ready?*, DENTONS (Mar. 19, 2021), *available at* https://www.jdsupra.com/legalnews/china-s-gdpr-is-coming-are-you-ready-4102991/.

[111] Gil Zhang & Kate Yin, *A look at China's draft of Personal Information Protection Law,* IAPP (Oct. 26, 2020), https://iapp.org/news/a/a-look-at-chinas-draft-of-personal-data-protection-law/.

[112] Personal Data Protection Act (PDPA) 2012 § 2, Law No. 26 of 2012, https://sso.agc.gov.sg/Act/PDPA2012.

[113] *Id.*

[114] Personal Data Protection Commission (PDPC) Singapore, Advisory Guidelines on Key Concepts in the Personal Data Protection Act (revised May 17, 2022), *available at* https://www.pdpc.gov.sg/guidelines-and-consultation/2020/03/advisory-guidelines-on-key-concepts-in-the-personal-data-protection-act (last visited Aug. 19, 2022); *see also* PDPA, *supra* note 112, § 15.

[115] PDPA, *supra* note 112, § 3.

[116] *See, for example,* Advisory Guidelines on Key Concepts in the Personal Data Protection Act, *supra* note 114.

III. PRACTICE POINTS

The following eight practice points are offered to help organizations and counsel navigate international legal holds that may potentially conflict with international data protection laws. Given that many international data protection laws appear to be based in whole or part on the GDPR and that the U.S. arguably has the most significant preservation requirements, the practice points are focused solely on the interplay between U.S. legal holds and the GDPR. The broader goal remains, however, to provide a framework for counsel implementing international legal holds wherever they may arise and that may conflict with international data protection laws, including but not limited to the GDPR.

1. Determine Whether the Preservation of Personal Data Is Necessary, and Then Determine Whether a Data Protection Law Applies

Once the duty to preserve has been triggered, an organization should promptly identify sources of discoverable information that may need to be preserved. Since most data protection laws focus on personal information, the first step is to analyze whether personal information must be preserved.

As discussed in Section II.B, personal information under many data protection laws is broadly defined. Thus, personal information is almost always contained within the sources of information to be preserved. There are certain data sources, however, that are not likely to contain personal information, including software, technical drawings, measuring or construction data, controller's financial data, marketing material, or public communications material. If preservation in a matter is limited to these types of information, it may be possible that preservation would not give rise to data protection obligations.[117] This would only be true, however, if there were no personal information at all included in the materials.

If personal information must be preserved, the next step is to assess whether another nation's data protection law applies to the data to be preserved. As discussed in Section II.B, the GDPR protects the personal information of natural persons who are in the EU and looks to controllers and processors to enforce its requirements. Controllers and processors are subject to the GDPR's requirements if they do business in the EU or they are based outside the EU but offer goods and services to, or monitor, individuals in the EU. Thus, to determine whether the GDPR applies to a U.S. legal hold, organizations must first identify the controller of the personal information to be preserved and determine whether the controller is subject to the GDPR.

[117] There may be other local laws or regulations, as well as contractual obligations, that impact decisions on processing and subsequent data transfer, including trade secret laws. Thus, counsel should consider consulting local counsel.

2. Apply the Data Protection Law's Guiding Principles for Processing Personal Information to Every Preservation Step or Process

As discussed in Section II.C.2, Article 5 of the GDPR sets forth guiding principles that govern the processing of personal information. The GDPR's principles include the requirements of:

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality; and
- Accountability.

These principles contain objectives for the design of data processing systems and the implementation of data processing operations.[118] Under the GDPR, these principles are a necessary element of each and every step in the scoping, implementation, maintenance, and eventual release of a legal hold. Thus, when implementing a legal hold, counsel should consider how the data protection principles will impact each step of the preservation process.

As noted in the introduction, this *Commentary* does not address cross-border data transfers. Nevertheless, the GDPR imposes additional requirements when transferring data outside of the EU/EEA or to jurisdictions that lack an adequacy determination.[119] Thus, under the GDPR, data should ideally be preserved in its native repository (preserved "in place") or copied and retained within jurisdictions deemed to have adequate privacy protections, and practitioners should exercise caution when transferring data across borders.[120]

---

[118] Roßnagel, in: SIMITIS, ET AL., *supra* note 33, Art. 5, Rz. 21.

[119] *See* GDPR, *supra* note 1, Chapter 5, arts. 44–50.

[120] *See* The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)* (Jan. 2017), available at https://thesedonaconference.org/publication/International_Litigation_Principles [hereinafter *International Litigation Principles*]. (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.").

3. Document the Lawful Basis for Preservation and Preservation Steps Taken Thereafter

A key GDPR principle that all controllers must adhere to when taking preservation steps is the accountability principle. GDPR Article 5(2) states:

> The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').[121]

Thus, to comply with the principle of accountability under the GDPR, counsel should document each step in the preservation process.[122] Documentation created and maintained by the controller or its designee should address:

1. What information is subject to preservation;
2. The purpose for preservation;
3. The proposed length of preservation;
4. The measures taken to communicate preservation decisions to the affected data subjects;
5. The measures taken to protect the information from unlawful use or disclosure, including security measures;[123] and
6. Communications with data protection officers or other authorities about the preservation efforts.[124]

The documentation can be maintained in a variety of formats but is most often kept in spreadsheets or in software designed for that purpose.

The controller should initially document the circumstances establishing that the duty to preserve has been triggered. Documentation should begin as soon as the preservation obligation has been triggered. The lawful basis for preservation, to the extent it differs from the triggering event, should also be recorded.

---

[121] GDPR, *supra* note 1, Art. 5(2).

[122] *See* European Data Protection Supervisor, *Accountability,* https://edps.europa.eu/data-protection/our-work/subjects/accountability_en (last visited Aug. 19, 2022).

[123] Data security is always a consideration when collecting ESI for a legal hold, particularly if that data is being copied and removed from its protected, secure native environment. The Sedona Conference Working Group 11 has published multiple papers providing guidance on this topic, which are available at https://thesedonaconference.org/publications under the section labeled "Data Security and Privacy."

[124] *See, e.g.*, EUROPEAN DATA PROECTION SUPERVISOR, LEADING BY EXAMPLE: EDPS 2015-2019, *available at* https://op.europa.eu/webpub/edps/edps-2015-2019-report/en/ (last visited Aug. 19, 2022).

The principle of accountability continues to apply after a lawful basis has been established.[125] This principle requires controllers to continue to document their decision-making in connection with each step of the preservation process.[126] In each case, the documentation should describe the preservation alternatives considered and the rationale for selecting one route over another.[127]

Documentation provides an effective means to defend the organization's actions should they be questioned at a later time. Further, documentation is necessary not only for potential review by the data protection authority but also to respond to data subject inquiries about whether personal information is being processed.[128] As noted earlier, counsel should consider using technology to be able to track and respond to requests in a timely manner.

4. Take Steps to Minimize the Scope of Preserved Information

Minimization is one of the GDPR's leading principles and allows information to be processed only if it is "adequate, relevant," and specifically limited to achieve the intended purpose.[129] For example, instead of reflexively placing a custodian on legal hold because of his or her title or department, counsel may—through interviewing, reviewing organizational charts, or taking other steps—consider whether the individual's information really has significance regarding the matter before placing the custodian on legal hold. Counsel may also prioritize certain custodians' sources or limit the particular sources that need to be preserved rather than automatically deciding that all of a custodian's sources should be preserved. Similarly, some litigants employ "preservation in place" strategies such as suspending the auto-delete function in an email system for identified custodians.[130] Although this last step still constitutes processing within the meaning of the GDPR, it at least reduces the overall exposure of the information to other parties. Another approach is to remove custodians' rights to alter or delete documents in their possession or control. And yet a third approach is to rely

---

[125] *See, e.g.*, UK GUIDE TO GDPR, *supra* note 83, *Accountability and governance*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/ (last visited Aug. 19, 2022).

[126] *See generally* Robert Healey, *GDPR and the Accountability Principle*, FORMITI (Aug. 10, 2022), https://formiti.com/gdpr-and-the-accountability-principle/.

[127] *Id.*

[128] *See* GDPR, *supra* note 1, art. 15 (*Right of access by the data subject*).

[129] *See* GDPR, *supra* note 1, art. 5(1)(c): personal information shall be: "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')."

[130] Some may argue that suspending the auto-delete function in order to achieve preservation may be in conflict with the minimization principle. Wherever possible, auto-delete functions should be suspended specifically for the relevant information subject to litigation hold such as individual mailboxes. Custodians would still have the ability to manually manage and delete content unrelated to the legal hold, thus ensuring minimization. *See* GDPR, *supra* note 1, art. 17 (1)(a), Recital 65: allowing the further retention of the personal data that is no longer necessary in relation to the original purposes but necessary for legal defense.

on custodians to take action to preserve information in their possession, custody, or control.[131] Although these last steps still constitute processing within the meaning of the GDPR, they at least delay the exposure of the information to other persons unless and until it is needed, and in some cases it may become unnecessary to collect the data if it turns out to be irrelevant or otherwise immaterial.

Some U.S. litigants, due to cost, burden, proportionality, and business interruption reasons, already take minimization concepts into account when preserving information under U.S. law.[132] Litigants who are not already using these more deliberative preservation strategies in the U.S. generally should consider employing them when preserving personal information that is subject to the GDPR to comply with the GDPR's minimization principle.[133] Furthermore, under minimization principles, counsel should consider reserving collection of or copying information for preservation purposes to those extreme situations where it is absolutely necessary—for example, where the information is in the hands of a bad actor likely to destroy relevant information. In such cases, the reason for preservation should be documented thoroughly and be based on principles of minimization.

5. Consider Involving Data Protection Officers, Supervisory Authorities, or Work Councils

Under the GDPR, data protection officers are appointed by controllers to advise on and monitor GDPR compliance. A data protection officer may be either an employee or an external service provider such as external legal counsel. The data protection officer holds a somewhat independent position and acts as the contact between controller and the supervisory authority.[134]

---

[131] Various authorities have confirmed that parties can rely on the good-faith actions of their employees in the preservation process so long as the process is properly supervised by case counsel. *See* Radiologix, Inc. v. Radiology & Nuclear Med., LLC, No. 15-4927-DDC-KGS, 2019 WL 354972, at *11 (D. Kan. Jan. 29, 2019) (producing party's reliance on custodians for identification and collection along with counsel's supervision of the process was appropriate and court "declines to conclude—in hindsight—that plaintiffs should have used different collection or searching methods to identify and produce relevant documents before trial"); *see also* New Mexico Oncology & Hematology Consultants, Ltd. v. Presbyterian Healthcare Servs., No. 1:12-cv-00526 MV/GBW, 2017 WL 3535293 (D.N.M. Aug. 16, 2017) (litigation hold effectuated through self-preservation not inadequate where custodians "were directed to retain documents and data 'that mention or discuss or relate to any of' an exhaustive list of subjects" and were "also directed that if 'you are unsure about the relevance of a document, be cautious and preserve it'"); *Sedona Commentary on Legal Holds, Second Edition*, *supra* note 4, at 408. ("[I]n most cases, a careful combination of notification as described above, collection, and individual action should enable parties to rely on the good-faith actions of their employees").

[132] *See Sedona Commentary on Legal Holds, Second Edition*, *supra* note 4, at 389 (Guideline 7: "Factors that may be considered in determining the scope of information that should be preserved include the nature of the issues raised in the matter, the accessibility of the information, the probative value of the information, and the relative burdens and costs of the preservation effort.").

[133] *See* GDPR, *supra* note 1, art. 5(2): "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

[134] *Id.* at art. 39, Recital 97 (*Data protection officer*).

The GDPR requires controllers to involve data protection officers in a timely manner when issues arise relating to the protection of personal information, including issues relating to a controller's legal hold process developed to comply with U.S. law.[135] Practically speaking, however, involving data protection officers in the legal hold process would only come into play in limited circumstances. Controllers are more likely to involve data protection officers with nonroutine preservation issues to obtain guidance and insight into formal or informal opinions of supervisory authorities[136] and/or obtain helpful indications on the interpretation of local laws. Controllers may also decide to involve a data protection officer in some matters because it may reflect well on the organization's commitment to protecting the rights of data subjects.[137]

Because some jurisdictions in the EU have strict labor laws and rules on employee representation, many organizations have agreements that detail the legal hold process in connection with employee rights.[138] Where appropriate, counsel should consult local counsel regarding the existence of local agreements prior to taking preservation steps in connection with a matter. Even in the absence of such an agreement, counsel should consider seeking guidance from the local works council[139] or other employee representatives before a legal hold is issued. This demonstrates transparency and also helps ensure a consistent and reasoned response from the organization should the employee reach out directly to the works council or employee representatives for guidance.

Early notice also enables the works councils to exercise their rights in an informed manner, which further protects the data subject's rights.[140] In some jurisdictions, employees have the right to ask for the presence of a works council member during legal interviews, such as during preservation interviews. This is particularly important if the individual could be subject to discipline in connection with the matter.

---

135 *Id.* at art. 38.

136 Data protection authorities frequently issue advice or practical tips on their websites or publish instructive articles in law journals on their interpretation of the law.

137 *International Litigation Principles*, *supra* note 120.

138 Under German law, a company can negotiate an agreement with the collective works council laying out in great detail specific processes, including details on issuance of a legal hold.

139 A works council is an institutionalized employee representation body in companies and corporate groups that represents the co-determination body under works constitution law. In Germany, by law, the works council resulting from a works council election is the representative of the workforce. *See* Betriebsverfassungsgesetz [BetrVG] [Works Constitution Act 1972], § 1. Counsel should keep in mind that various forms of employee representations exist in different countries.

140 GDPR, *supra* note 1, Recital 60 (*Information obligation*) highlights that the principle of *fairness* requires controllers to provide the data subject with any further information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal information is processed.

6. Communicate Clearly with Data Subjects, Advising What Materials the Organization is Preserving, and What Steps Will be Taken as to Personal Information

Giving notice to affected individuals that their information is being preserved pursuant to a pending U.S. legal matter is a key requirement of the GDPR.[141] Under the GDPR, data subjects must receive notice that personal information is being processed, the reasons for preservation (processing), an explanation of their rights, and a means to exercise their rights.[142]

More specifically, GDPR Article 13(1) requires that the following information be provided where personal information is collected from the data subject:

> (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
>
> (b) the contact details of the data protection officer, where applicable;
>
> (c) the purposes of the processing for which the personal information is intended as well as the legal basis for the processing;
>
> (d) the legitimate interests pursued by the controller or by a third party;
>
> (e) the recipients or categories of recipients of the personal information, if any; and
>
> (f) where applicable, the fact that the controller intends to transfer personal information to a third country or international organisation.

The principle of *transparency* requires that such information be easy to understand.[143]

Controllers likely already have in place general information regarding their processing practices, such as a privacy notice for employees. These general notices may only address processing that occurs in the regular course of business in an employment context and not fully describe all aspects of processing needed for preservation in a U.S. legal matter. Counsel should consider issuing matter-specific notices, written in clear and simple language, to communicate with data subjects about preservation. An example of a notice that incorporates the GDPR's requirements is attached as Appendix A.

---

[141] In exceptional cases, the duty to inform does not apply. Such cases include situations where the notice about the intended further processing would interfere with the establishment, exercise, or defense of legal claims and where the controller's interest in not providing the information outweighs the data subject's interest. *See, e.g.,* Germany's Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], June 30, 2017, § 32.

[142] GDPR, *supra* note 1, art. 13(1).

[143] *See supra* Section II.C.2.

Many organizations handle the notification described above by addressing it in written legal hold notices. Under these circumstances, the legal hold notice should include information about the privacy rights of the data subjects and use of their personal information.[144] Referring to FAQ documents or other internal reference materials relating to legal holds that help a custodian better understand what is being asked of them when responding to a legal hold notice can also demonstrate transparency and consistency.

Notice should be provided as quickly as possible.[145] Under the GDPR, notice should be provided upon or before the commencement of any preservation activities.[146]

In fulfilling preservation obligations, counsel should be aware that not all jurisdictions recognize that legal hold notices or related communications are protected by the attorney-client privilege or work-product doctrine. U.S. courts typically find that legal hold notices are protected by the attorney-client privilege and the work-product doctrine.[147] In contrast, jurisdictions outside the U.S. that recognize similar concepts of attorney-client privileged communications or attorney work product do not typically consider legal hold notices or preservation steps to be privileged except when external

---

[144] Counsel should consider referencing GDPR Article 5 principles for the protection of personal information. Counsel should also recognize the conflict between U.S. preservation law and EU law on the required preservation of relevant personal information. Pursuant to Rule 34 of the Federal Rules of Civil Procedure, some U.S. courts have required organizations to preserve potentially relevant personal webmail of employees and/or the potentially relevant text messages stored on personal mobile devices on the theory that corporations are deemed to have control over their employees work-related documents, whether located at the office or at home. Paisley Park Enters., Inc. v. Boxill, 330 F.R.D. 226 (D. Minn. 2019) (finding defendants failed to preserve relevant text messages from executives' personal devices used for company business); Fluke Elecs. Corp. v. CorDEX Instruments, Inc., No. C12-2082JLR, 2013 WL 566949, at*13 (W.D. Wash. Feb. 13, 2013) (noting that litigants owe a duty to preserve what they know or reasonably should know will be relevant evidence, including ESI from personal and home computers and other devices); Helmert v. Butterball, LLC, No. 4:08CV00342 JHL, 2010 WL 2179180, at *9 (E.D. Ark. May 27, 2010) (ordering corporation to produce email from personal email accounts from upper management employees over the corporation's objection that it did not have access to the employees' accounts). German civil law states that upon termination of the employment relationship, an employee must return all business documents that have been made available by the employer or the employer's representative (so called "duty to return," *see* BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE], § 667, alt. 1, as well as those which the employee has obtained during the employment relationship, *e.g.*, through correspondence with a third party, *id.* § 667, alt. 2; files, other documents, and files that the employee has prepared himself in connection with his work, as well as copies of such documents, must also be returned (*See* Bundesarbeitsgericht [BAG] [Federal Labor Court], Dec. 14, 2011, NZA 2012, 501; Christoph Bergwitz, *Zurückbehalten von Geschäftsunterlagen*, NZA 2018, 333). However, this duty to return does not give the employer the right to demand surrender of the employee's entire private device, which he may have used to create such communication or files.

[145] *See also* The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, 17 SEDONA CONF. J. 397, 409 (2016) (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.").

[146] GDPR, *supra* note 1, art.13(1).

[147] Typically this protection is based on the attorney-client privilege and the work-product doctrine. *See* Gibson v. Ford Motor Co., 510 F. Supp. 2d 1116, 1123–24 (N.D. Ga. 2007).

counsel are involved.[148] Organizations should consider whether outside counsel should draft the legal hold notice and be consulted on preservation steps.

7. Make Sure Legal Hold Notices are Translated in Accordance with Local Law

Local laws may require that "business communications" or "employee communications" be translated.[149] It is not always clear whether a legal hold notice constitutes a "business communication" requiring translation. The conservative approach is to treat a legal hold notice as a business communication and incorporate translations when appropriate.[150]

Translation of a legal notice into the native language of the recipient is consistent with the GDPR principle of transparency. Moreover, many Civil Code jurisdictions require that business documents be translated into an individual's primary language.[151] Belgian law, for example, requires that business documents between employer and employees be provided in Dutch, French, or German, depending on the individual's primary language.[152] Likewise, France requires that business documents between employer and employee be in French.[153] While Civil Code jurisdictions tend to have laws requiring translation of certain business and/or employee communications into native languages, common law jurisdictions generally allow business communications to be in English and do not have strict statutory translation requirements. Counsel should consider consulting with local counsel regarding appropriate interpretation of the local laws and their application to legal hold notices.

Even when not required, providing legal hold notices in the recipient's native language can help ensure that recipients understand the notice. It is also important to consult and follow the organization's internal policies on translation of business communications.

---

[148] For example, Japan does not currently protect "communications between a corporation and non-*bengoshi* in-house lawyers [i.e., in-house counsel]." Masamichi Yamamoto, *How Can Japanese Corporations Protect Confidential Information in U.S. Courts?*, 40 VAND. J. TRANSNAT'L L.503, 515 (2007).

[149] Providing hold instructions in a native or local language can also foster better understanding and demonstrate good faith in addressing preservation obligations. For example, in *E.I. du Pont de Nemours & Co. v. Kolon Industries*, a dispute arose after non-English speaking employees were found to have spoliated relevant information. The court ultimately imposed sanctions, finding that the company had failed to affirmatively monitor compliance by non-English speakers with a legal hold notice issued in English. 803 F. Supp. 2d 469, 479 (E.D. Va. 2011). The legal hold notice was written in English and distributed mostly to non-English speaking employees of a South Korean company (in addition to its United States subsidiary). Ultimately, the Court imposed sanctions in the form of attorneys' fees, expenses, costs, and an adverse inference instruction. *Id.* at 510.

[150] Belgium, France, Québec, Spain, Mongolia, Kuwait, Saudi Arabia, Turkey, Slovakia, Poland, and Venezuela are a few jurisdictions with local laws governing employee communications.

[151] UK GUIDE TO GDPR, *supra* note 83, *How should we draft our privacy information?*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/how-should-we-draft-our-privacy-information/ (last visited on Aug. 19, 2022).

[152] Decree of the Vlaamse Gemeenschap [on the use of languages] of July 19, 1973, BELGISCH STAATSBLAD [Official Gazette of Belgium], Sept. 6, 1973, 10089.

[153] *See* CODE DU TRAVAIL [C. TRAV.] [LABOR CODE] art. L.1321-6.

8. Reevaluate and Release Legal Holds and Dispose of Information When No Longer Needed

As a matter progresses, the scope of a legal hold may change, expanding in some cases and narrowing in others. When it does, organizations subject to a U.S. legal hold are expected to reevaluate the scope of the hold notice and amend it as necessary.[154] This is particularly important for legal holds involving personal information subject to the data protection law. For example, failing to address changes to the scope of the legal hold could violate three key GDPR processing principles: "purpose limitation," "data minimisation," and "storage limitation."[155]

Under the GDPR, the purpose limitation requires that personal information be collected only "for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."[156] Personal information that has been placed on legal hold and preserved cannot be processed for any other purpose. If the scope of the matter changes, the controller must evaluate whether the original purpose still exists or if other matters or issues can support the original purpose. If the original purpose no longer exists, or the matter has terminated, then the GDPR requires that the legal hold be terminated and the personal information released from the hold.[157] Changes in scope may require the controller to revise the notice.

The principle of data minimization under the GDPR also limits the use of personal information to "what is necessary in relation to the purposes for which they are processed."[158] Organizations should release a legal hold and dispose of personal information collected for preservation but later determined not to be discoverable. This can include information that was culled based on search criteria that have not been challenged or has been agreed to by opposing counsel, and no future challenge is anticipated.

---

[154] Guideline 8(f) of the Legal Hold Guidelines recommends that legal hold notices be "periodically reviewed and amended when necessary." *Sedona Commentary on Legal Holds, Second Edition*, *supra* note 4, at 399.

[155] GDPR, *supra* note 1, art. 5(1)(b), (c), and (e).

[156] *Id.* at art. 5(1)(b).

[157] In 2019, the Berlin data protection commissioner had issued a fine notice of 14.5 million Euros against Berlin's largest private landlord. *See* https://openjur.de/u/2331402.html. This was the highest fine to date in Germany based on the GDPR. Deutsche Wohnen was fined because personal data of former tenants, such as social and health insurance data, employment contracts, or information about their financial circumstances, could still be viewed and processed via the company's archive, and the archive had no technical functionality to delete data. The authority had already drawn the company's attention to the irregularities in 2017 and demanded a remedy. The Berlin Regional Court declared the decision of the Berlin data protection commissioner to be invalid because it lacked details of specific acts. Subsequently, the public prosecutor's office, in agreement with the state data protection commissioner, filed an appeal before the Kammergericht, which in late 2021 turned to the European Court of Justice for guidance. Regardless of the outcome of the proceedings, it is clear that data protection authorities are prepared to impose heavy fines and are not afraid to exhaust legal remedies.

[158] GDPR, *supra* note 1, at art. 5(1)(c).

Under the principle of storage limitation, personal information must not be retained in a form that permits the identification of a data subject for any length of time that is "longer than necessary for the purposes for which the personal data are processed."[159] Accordingly, personal information that is no longer required to be preserved under a U.S. legal hold and is not otherwise needed by the organization must be released and/or any collected information destroyed as soon as possible once the information is no longer needed for the matter.[160]

[159] *Id.* at art. 5(1)(e).

[160] *See Sedona Commentary on Legal Holds, Second Edition*, *supra* note 4, at 408–09.

IV. CONCLUSION

Controllers or processors doing business in the EU or who offer goods or services to EU residents or monitor their behavior within the EU, and who are required to implement preservation steps as to data subjects' personal information pursuant to a U.S. legal hold, must comply with the requirements of the GDPR. We have provided eight practice points above to help counsel comply with the GDPR under these circumstances. The practice points should also provide a useful framework for counsel implementing international legal holds in other jurisdictions beyond the U.S. and that may have conflicting international data protection laws beyond the GDPR.

APPENDIX A

Sample Notice Incorporating GDPR Requirements

Dear [recipient],

[Company name] is involved in a matter [provide high level detail regarding investigation, lawsuit, etc.] pending in the United States District Court for the (detail court information).

By law, the company is required to preserve information that may be relevant and ensure that such relevant information is not modified or destroyed. You are receiving this notice because you may have relevant information regarding this matter. Information that must be preserved includes email and other types of electronic communications, documents (paper or electronic) or other electronically stored information and/or paper documents. Relevant information may also include personal information that may identify you, such as your name, email address, telephone number, or other personal identifiers.

The company has a legitimate interest in preserving your personal information to comply with its legal obligations in connection with the matter. The legal basis for processing your personal information is GDPR Art. 6 (I) (f). The personal information will be preserved until the matter is completely resolved and the company no longer has a legal obligation to preserve it.

To preserve the information, the company may take some or all of the following steps:

1. Search for information that may be relevant to the matter.

2. Make copies of any of the personal information described above.

3. Review information to determine whether it is relevant to the matter.

4. Create information about the personal information for analysis purposes and to help fulfill the company's legal responsibilities.

5. Share information with other company employees participating in the matter or with legal counsel or others hired with respect to the matter.

Depending on how the matter progresses and the company's legal responsibilities, the company may ultimately be required to transfer some of the preserved personal information to another country, including countries with no adequacy decision by the European Commission, for review by legal authorities or other counsel involved in the matter.

With respect to the processing of your personal information in this matter and to the extent granted by GDPR, you have the following rights:

1. The right to request information about, to access, or to receive copies of your personal information in a form readable by you;

2. The right to ask to correct personal information about you that is being preserved (which may be granted or not depending on the company's legal obligations);

3. The right to ask the company to delete certain personal information (which may be granted or not depending on the company's legal obligations);

4. The right to ask for restriction of processing;

5. The right to object to the preservation of personal information about you (which may be granted or not depending on the company's legal obligations);

6. The right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before withdrawal of consent;[161] and

7. The right to file a complaint about preservation of your personal information with the following supervisory authority: [name and contact information].

If you have any questions regarding this notice or wish to object to the preservation of your personal information, please contact the responsible controller at:

> [name of controller and contact person along with email, address and phone information.]

You may also contact the data protection officer at:

> [name of data protection officer and contact information, with explanation of who and why to contact either.]

The company will keep you advised regarding the progress of the matter and the preservation of your personal information. The company will also notify you when the matter is resolved and the company's obligation to preserve personal information has ended.

Thank you for your cooperation and understanding. If you have questions or concerns about this letter, please feel free to contact:

[Contact information of the writer or other suitable person]

Signed
Title

---

[161] *See* GDPR, art. 13 (2) (c). Only add in cases where processing is based on consent from the data subject.