

# *Cross-Border Legal Holds: Challenges and Best Practices*

*James A. Sherer and Taylor M. Hoffman*



# Cross-Border Legal Holds: Challenges and Best Practices

by James A. Sherer, BakerHostetler and Taylor M. Hoffman, Swiss Re, with Practical Law Litigation

**Maintained** • International, USA (National/Federal)

---

*This Practice Note details key considerations and best practices for implementing a US-style legal hold abroad, including how to craft a cross-border legal hold policy and process and the main steps involved in issuing and executing a cross-border legal hold.*

---

## Crafting a Cross-Border Legal Hold Policy and Process

Jurisdictional Differences on the Scope of Discovery

Foreign Data Privacy Restrictions

## Implementing a Cross-Border Legal Hold

Determining When to Issue a Legal Hold

Identifying Relevant Information and the Scope of Preservation

Drafting a Legal Hold Notice

Maintaining a Legal Hold

Reviewing Relevant Organizational Policies

## Best Practices for Cross-Border Legal Holds

The US recognizes what is likely the broadest discovery standard for civil litigation in the world. When a multinational organization with global operations and information confronts a US-based investigation or litigation matter, it must consider how best to implement an appropriate US-style **legal hold** in its international locations in the face of conflicting obligations imposed by foreign jurisdictions.

Simply put, a US-style legal hold requires the preservation of information relevant to an investigation or a litigation, regardless of where the information resides. Organizations typically send legal holds when they reasonably anticipate an investigation or a litigation to instruct individuals, including officers and employees, about their obligation to preserve relevant information. Issuing a hold also typically includes suspending the organization's routine document destruction practices.

While many practitioners are familiar with implementing legal holds domestically, legal holds for an organization with a global footprint require special care. This Note explores key considerations and best practices for:

- Crafting a policy or process for cross-border legal holds, including jurisdictional differences on the scope of discovery and data privacy requirements (see [Crafting a Cross-Border Legal Hold Policy and Process](#)).

- Planning, documenting, and implementing a US-style legal hold to preserve information and documents abroad (see [Implementing a Cross-Border Legal Hold](#)).

## Crafting a Cross-Border Legal Hold Policy and Process

Under [Federal Rule of Civil Procedure \(FRCP\) 26\(b\)\(1\)](#) and similar state rules of practice, parties must apply proportionality to all aspects of discovery, including the preservation of information relevant to an investigation or a litigation. Courts determine a party's discovery and preservation conduct in light of proportionality (see, for example, [Rimkus Consulting Grp. v. Cammarata](#), 688 F. Supp. 2d 598, 613 (S.D. Tex. 2010)). Proportionality considerations in the US include, among other things:

- The importance of the issues at stake (and the importance of the action or investigation generally).
- The amount in controversy.
- The parties' relative access to relevant information.
- The parties' resources.
- The importance the information plays in resolving the issues.
- The balance between the burden and expense of the proposed discovery and the likely benefit of the information.

([FRCP 26\(b\)\(1\)](#).)

Yet even with proportionality considerations, the scope of discovery and related legal hold obligations in the US is far broader than what most foreign jurisdictions permit. Specifically, many foreign jurisdictions have stringent data privacy protections that US organizations must take into account when planning and implementing a legal hold. To ensure that cross-border legal holds adequately address these jurisdictional differences, multinational organizations should adopt appropriate best practices for their organization (see [Box, Best Practices for Cross-Border Legal Holds](#)).

## Jurisdictional Differences on the Scope of Discovery

The differing regulatory regimes and cultural approaches to data protection have some bearing on legal holds generally (see [Foreign Data Privacy Restrictions](#)). However, the discovery conflicts between and among jurisdictions may have a more immediate impact on organizations implementing cross-border legal holds. This impact is clearest for non-US individuals assisting with cross-border legal holds, where the difference between the US-based legal hold for which they are preserving information may dramatically differ in character and scope from the foreign proceedings they are used to. The key differences stem from whether a country's legal system is:

- **A civil law regime.** Most civil law jurisdictions have a restrictive approach to discovery and often have no formal discovery process. These jurisdictions limit discovery to only what is needed for the scope of the trial and prohibit additional disclosure. In fact, in some regimes, such as Germany, an organization generally must disclose documents that it intends to use to advance its own case, and it need not disclose documents undermining the merits of its case. Most member states of the European Economic Area (EEA) and the majority of other countries around the world, ranging from Azerbaijan to Benin, Cote d'Ivoire to China, and Russia, Guatemala, and parts of India, use civil law regimes that do not require US-style discovery ([Art. 29 Data Prot. Working Party, Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation](#), at 4-5, Doc. No. 00339/09/EN WP 158 (Feb. 11, 2009) (Art. 29 Working Party)).
- **A common law regime.** Common law countries, such as Australia, Canada, Hong Kong, Singapore, and the United Kingdom, sometimes recognize or contemplate broader discovery than the disclosure available in civil law jurisdictions. In comparison to the broad US approach to discovery, however, common law regimes severely restrict the scope of pretrial discovery and related access to information.
- **A combined religious and civil code regime.** Some countries use a mix of religious codes and other legal systems. For example, Egypt's legal system combines Sharia (Islamic) law and a civil and commercial code system, while Nigeria's legal system combines pre- and post-Colonial common law, customary law based on traditional norms and practices, and Sharia law.

Some civil law jurisdictions have enacted blocking statutes to prevent the collection and use of information in cases outside of that country, in part because of the different approaches between common and civil law countries. However, when these blocking statutes are implicated in US litigation, conflicts of laws can result. An organization must balance the risk of failing to satisfy US discovery obligations with the risk of committing a statutory violation in the foreign country. One way to minimize these concerns is to preserve information in-country (and minimize transfers) to the extent possible.

## Foreign Data Privacy Restrictions

Foreign approaches to data privacy affect the scope of preservation outside of the US. The EEA, through the European Union (EU) General Data Privacy Regulation (Regulation (EU) 2016/679) (GDPR), which went into effect in May 2018, codifies a fundamental right to the protection of citizens' data privacy in a way that differs from both the US-sectoral data privacy approach as well as certain state-specific regulations (such as the California Consumer Privacy Act or CCPA). For example, in the US, "personal data" typically refers to specific types of data, such as personal financial information or health information protected by the [Health Insurance Portability and Accountability Act](#) (HIPAA). By contrast, "personal data" in the EU carries a much broader meaning and includes any information that may identify an individual, and regulations (such as the CCPA) go even further and may include information identifying households and devices. (For information on UK data protection law after the Brexit transition period, see [Practice Notes, Brexit post-transition period: data protection \(UK\)](#) and [Brexit: implications for data protection.](#))

Organizations should review foreign blocking statutes and data privacy laws together to determine whether they can claim legitimate reasons for the preservation and subsequent collection and use of the information at issue. Whether foreign restrictions are framed as privacy laws, blocking statutes, or state or bank secrecy considerations, most of these data protection laws limit an organization's ability to:

- Process an individual's personal data without the individual's consent (see [Processing Personal Data](#)).
- Transfer an individual's personal data outside the home country to a country that the home country considers inadequate in its protection of personal data (see [Transferring Personal Data](#)).

### Processing Personal Data

While the preservation of information may not seem to implicate European or other data privacy rules at first blush to a US-based attorney, preservation of information, even in place, may qualify as processing.

For example, the GDPR defines data processing significantly broader than what is commonly understood as processing in the US. Specifically, the GDPR defines processing as "any operation or set of operations" performed on personal data that involves, among other things, collection, recording, organization, storage, retrieval, disclosure by transmission, dissemination, or destruction (GDPR, art. 4(2)). This definition is potentially broad enough to implicate an organization's legal hold.

Accordingly, an organization that must implement a legal hold at locations within the EU should determine whether the legal hold is permissible under one of the following exceptions:

- The data subjects of the hold unambiguously consent to the processing of their personal data (GDPR, art. 6(1)(a)).
- The organization, as the controller of the information, must process the personal data for its own or a third party's legitimate interests (GDPR, art. 6(1)(f)).

While broad in theory, these exceptions are tricky in practice. For example, if an organization seeks an exception based on its own legitimate interest, such as an interest in complying with US discovery obligations, a European court may not read "legitimate interests" as broadly as a US court, given both the civil law approach of document disclosure within the EU and the EU's perception of US regulatory overreach.

Moreover, EU regulators have tended to view exemptions based on employee consent skeptically and questioned whether an employee can truly give consent when the employee's job may be on the line (Art. 29 Working Party, WP 114, at 11). Further, employee custodians may withdraw their consent at any time, making internal efforts to preserve information more complicated (Art. 29 Working Party, WP 48, at 23).

For more information on the GDPR's requirements for obtaining valid consent and processing an employee's personal data, see [Practice Note, Employee Consent Under the GDPR](#).

Therefore, when an organization's legal hold might implicate employee data preservation outside of the US, an organization with a Data Privacy Officer (DPO) should consult the DPO when creating legal hold practices and policies. An organization might also consider involving an employee works council in the legal hold policy planning process to reach an understanding on what procedures the organization will employ when implementing a legal hold.

### Transferring Personal Data

Practitioners should preserve information in-country to the extent possible. However, practitioners taking this approach should note that transfers still may be unavoidable as part of the preservation process, such as when:

- A US-based legal hold implicates technology or information held in a country where operations are winding down.
- Current technological infrastructure or personnel are inadequate to properly effectuate preservation.
- Information is improperly located in a foreign jurisdiction, for example, if the information was transferred in contravention of:
  - the US Export Administration Regulations (EAR) that govern the export of software and technology;
  - the International Traffic and Arms Regulations (ITAR) that govern the export of controlled technical data; or
  - the [Office of Foreign Assets Control](#) (OFAC), which restricts exports to targeted countries and people.

While the focus of this Note is limited to preserving information abroad, and does not address the collection or review of that preserved information, preservation practices that require or implicate transfers can also raise questions about whether personal data was transferred in accordance with foreign law. These questions are especially relevant where an organization has the right or ability to access information in a foreign jurisdiction, but accessing that data would implicate blocking or related statutes. This cross-border access (and, therefore, transfer) could occur when data is located in a jurisdiction with stringent privacy protections and prohibitions against transfers to jurisdictions without such protections, but the data is in danger of [spoliation](#) if it is not transferred. In these cases, practitioners should perform a balancing test to determine the extent of necessary preservation and how the preservation will be performed.

### Implementing a Cross-Border Legal Hold

Implementing a legal hold typically includes the following steps:

- Determining when the organization should issue the legal hold (see [Determining When to Issue a Legal Hold](#)).

- Identifying relevant information, including key custodians and data locations (see [Identifying Relevant Information and the Scope of Preservation](#)).
- Drafting and circulating a legal hold notice (see [Drafting a Legal Hold Notice](#)).
- Maintaining the legal hold and preserving relevant information, as well as releasing the legal hold and returning the implicated data to its regular retention schedule (see [Maintaining a Legal Hold](#)).
- Determining which other organizational policies are potentially implicated by the legal hold (see [Reviewing Relevant Organizational Policies](#)).

## Determining When to Issue a Legal Hold

An organization should issue a legal hold when it reasonably anticipates litigation or an investigation if there is potentially relevant information (evidence) that the organization might otherwise delete, destroy, or lose. This moment, sometimes called the RAL (reasonable anticipation of litigation), requires some degree of legal judgment informed by both:

- **Objective factors.** These factors include:
  - the receipt of a summons or complaint;
  - the issuance of a [subpoena](#);
  - a formal notice that an organization is the target of an investigation;
  - the filing of a regulatory agency charge;
  - a legal hold letter from opposing counsel; or
  - a request to retain counsel to draft a complaint on behalf of the organization (as opposed to a request to merely assess the merits of a potential claim).
- **Subjective factors.** Depending on the nature of the dispute, these factors might include, for example:
  - a complaint from a customer with a history of litigation against the organization;
  - a threat from a competitor, when combined with circumstances known internally; or
  - a relatively serious internal complaint relayed by a supervisor.



The RAL triggers an organization's requirement to timely issue a legal hold, the timing of which may be critical in instances where an organization has automatic processes that delete potentially relevant information as a matter of course (*Apple, Inc. v. Samsung Elecs. Co.*, 881 F. Supp. 2d 1132, 1145, 1150 (N.D. Cal. 2012); see also *Berrios v. Jevic Transp., Inc.*, 2013 WL 300889, at \*4-5 (R.I. Super. Jan. 18, 2013) (finding that a RAL arose within hours of a fatal motor vehicle accident because the defendant was aware that fatal accidents are "likely [to] engender litigation")). Generally speaking, however, it is not feasible to immediately implement a legal hold given the steps involved to identify potential relevant data and custodians.

Additionally, practitioners must keep in mind that multinational organizations are sometimes plaintiffs in actions. A plaintiff organization generally must preserve information and issue a legal hold when it determines that it will file suit rather than waiting to implement a hold at the time it files a complaint or serves an adverse party (see, for example, *Apple Inc. v. Samsung Elecs. Co.*, 888 F. Supp. 2d 976, 997 (N.D. Cal. 2012)).

When an organization is more likely than not to initiate litigation, it has a duty, acting reasonably and in good faith, to take effective steps to preserve relevant information (see *In re Delta/AirTran Baggage Fee Antitrust Litig.*, 770 F. Supp. 2d 1299, 1312 (N.D. Ga. 2011)). If the organization does not preserve information and the information is lost, an adverse party may ask the court to impose sanctions for spoliation. Federal courts determining sanctions for spoliation typically consider:

- The effectiveness of the organization's preservation efforts.
- The documented preservation efforts and whether that evidence supports sanctions under [FRCP 37\(e\)](#).

(See 2015 Advisory Committee's Note to [FRCP 37\(e\)](#).)

For more information on the factors counsel should consider to determine when a party should have reasonably anticipated litigation, triggering its duty to preserve relevant documents and **electronically stored information** (ESI), see [Practice Note, Reasonable Anticipation of Litigation Under FRCP 37\(e\): Triggers and Limits](#).

For more information on spoliation sanctions under [FRCP 37\(e\)](#), see [Practice Note, Sanctions for ESI Spoliation Under FRCP 37\(e\): Overview](#).

## Identifying Relevant Information and the Scope of Preservation

Organizations must determine early on what information should be subject to a legal hold. Particularly for disputes with cross-border implications, organizations should try to limit the scope of preservation to only data that is relevant and necessary to support claims or defenses by:

- Identifying the custodians who are likely to have relevant information and should receive legal hold notices (see [Custodians](#)).



- Tracking the locations of relevant information, often through a data map (see [Data Maps](#)).
- Balancing any challenges or conflicts of laws posed by data processing restrictions in foreign jurisdictions (see [Conflicts of Laws](#)).

Identifying the scope of preservation is a key opportunity to ensure that the scope of the legal hold is proportionate to the matter. Given the hurdles of placing non-US data on hold, the proportionality requirement likely means that fewer non-US based custodians would be placed on hold than had they been based in the US.

### Custodians

The determination of the proper custodians and recipients of a legal hold is paramount. If a legal hold notice is distributed too narrowly, the organization risks failing to preserve important data and losing that data before it has a chance to retrieve it.

On the other hand, an overly broad legal hold can upend the organization's normal business practices to a degree that is disproportionate to the significance of the underlying investigation or litigation. Additionally, an organization that distributes a legal hold notice too broadly may risk conflicts with foreign data protection regulations (see [Foreign Data Privacy Restrictions](#)) or compromise an argument over the privileged status of the notice (see *United States ex rel. Barko v. Halliburton Co.*, 74 F. Supp. 3d 183, 190-92 (D.D.C. 2014); see [Drafting a Legal Hold Notice](#)).

To achieve the right balance, an organization can use early data assessment (EDA) and early case assessment (ECA) practices and technologies to consider all potential sources of responsive and relevant information (both system- and custodian-based). This can help the organization determine the substantive information it should preserve. Additionally, EDA and ECA workflows can eliminate some sources from further preservation efforts, which is particularly critical in cross-border situations.

For more information on EDA and ECA, including information on using these practices to identify relevant ESI for review, see [Practice Notes, The Advantages of Early Data Assessment](#) and [Case Assessment and Evaluation](#).

Key custodians who should automatically receive a legal hold notice fall into the following two categories:

- **Matter-specific custodians.** These individuals possess documents and evidence relating to the facts of the underlying dispute. In addition to evaluating current employees, an organization should consider:
  - looking into whether former employees might have possessed relevant information and, if so, determine whether that information remains in the organization's possession and can be preserved;
  - including legal hold inquiries in departing employees' exit interviews; and

- placing new employees who assume responsibilities for information relating to an existing legal hold on that hold.
- **General custodians or data stewards.** These individuals typically are in charge of systems, such as information technology (IT) assets, that store relevant information or records or documentation generally. They might also maintain:
  - electronic systems that store relevant data sets or types, including, for example, customer relationship manager (CRM) databases or former employee email;
  - other types of records, including libraries of documentation or warehouses of information or other off-site storage locations; or
  - information stored by third parties, on behalf of the organization, according to contract or corporate structure (such as another company within the same corporate umbrella).

Additionally, information may be in an organization's possession, custody, or control without residing on the organization's systems or with its employees. While there is conflicting case law on what constitutes "possession, custody, or control" when the organization does not have actual possession, third parties working at the direction of the organization might possess relevant information. The organization should consider providing third-party legal hold notices to these third parties.

For more information on discoverable ESI, including information on the traditional tests courts use to determine control over ESI in non-parties' possession and emerging jurisdictional issues relating to cloud-based ESI, see [Practice Note, Possession, Custody, and Control of ESI](#).

### Data Maps

Organizations often identify the key custodians and documents they must preserve by using a data map that identifies the substance, form, and location of information within the organization. In particular, a data map should identify systems that use automatic deletion mechanisms so that the organization can preserve any information stored on the implicated systems, or suspend the automatic deletion mechanisms, before additional information is lost.

Data maps can be an important tool for practitioners responsible for legal holds, especially when time is of the essence and counsel must determine whether (and to what extent) to preserve data residing outside of the US that might be subject to processing or disclosure limitations.

For more information on data mapping, see [How to Organize Company Data Before Litigation Arises Checklist](#).

### Conflicts of Laws

Organizations faced with competing (and sometimes inapposite) data processing requirements between countries may risk sanctions for their activities. For example, an organization's legal processing obligations in one country may be prohibited in another country. Because these rules are not harmonized, practitioners must consider the costs, risks, and burdens associated with legal hold activities in each interested country.

Although courts generally understand that these conflicts of laws exist, practitioners often submit documentation to the court explaining the conflicts. Once a dispute has matured into actual litigation, practitioners should seek appropriate stipulations and **protective orders**, as applicable, to provide order to the discovery process and to keep the parties focused on the immediate and proportionate discovery at hand. An organization should preserve data for only as long as necessary for the matter, and seek protective orders for the release of legal holds when appropriate.

Additionally, an organization might discuss the scope of information preservation and collection with investigators in government investigations or with opposing parties and courts in civil matters to avoid or minimize potential data privacy concerns associated with legal holds.

## Drafting a Legal Hold Notice

Most fundamentally, a legal hold notice should be comprehensive and clearly describe the information relevant to the investigation or litigation that the individuals and the organization must preserve. The notice should identify the substantive parameters of information that the organization must preserve in a straightforward manner so that the recipients, who often are not attorneys, can understand and abide by it. As a best practice, organizations typically distribute written legal hold notices rather than oral ones, even though a written notice is not necessarily required.

In addition to providing information on the dispute and instructions about complying with the legal hold, many legal hold notices also incorporate questionnaires that seek additional, individualized information from the custodians, including:

- A description of the relevant information that the custodian possesses.
- A description of the relevant information that the custodian knows about.
- The names of other custodians who may have relevant information and should be placed on the legal hold.
- Any questions the custodian has regarding the legal hold.

Organizations usually send legal hold notices by or at the direction of in-house attorneys or outside counsel. Involving attorneys in the legal hold process generally helps an organization to defensibly understand the scope of the investigation or litigation and craft the legal hold accordingly.

Additionally, language within the legal hold notice, when drafted by or at the direction of attorneys, may be protected from disclosure in discovery as **privileged attorney-client communications** and **work product**, depending on the jurisdiction (compare *Ingersoll v. Farmland Foods, Inc.*, 2011 WL 1131129, at

\*17 (W.D. Mo. Mar. 28, 2011) ("As a general matter hold letters are not discoverable, particularly when a party has made an adequate showing that the letters include material protected under attorney-client privilege or the work product doctrine.") and [Gibson v. Ford Motor Co.](#), 510 F. Supp. 2d 1116, 1123-24 (N.D. Ga. 2007) (finding that disclosure of information about the legal hold was "not reasonably calculated to lead to the discovery of admissible evidence") with [Boyington v. Percheron Field Servs., LLC](#), 2016 WL 6068813, at \*11 (W.D. Pa. Oct. 14, 2016) (finding that the defendant failed to show that information surrounding its preservation efforts was privileged and granting a motion to compel discovery of the facts surrounding the defendant's preservation efforts) and [Barko](#), 74 F. Supp. 3d at 190-92 (requiring disclosure of the defendant's legal hold notice, while acknowledging that "the question is a close one").

The individuals involved in drafting the legal hold notice generally should seek guidance from:

- IT and information governance resources within the organization. Individuals in these groups can also help explain to the legal department and outside counsel how the organization and its underlying systems and information governance practices work.
- Relevant business and organizational units, given the subject matter of a particular investigation or litigation. Individuals in these groups may have additional information about the facts involved in the underlying matter and who should receive the notice.

## Maintaining a Legal Hold

Often, the legal department appoints a representative to oversee the implementation and tracking of a specific legal hold. Among other oversight activities, this representative may need to:

- Coordinate with IT professionals to ensure that they deploy technological tools appropriately to preserve information (see [Coordinating with IT](#)).
- Confirm that custodians have received the legal hold notice and are complying with its instructions (see [Confirming Receipt](#)).
- Determine how the organization will handle redundant information possessed by multiple custodians (see [Handling Redundancy](#)).
- Modify or lift a legal hold as circumstances change (see [Modifying a Legal Hold](#)).

## Coordinating with IT

The individual responsible for maintaining the legal hold must confirm that the organization actually preserves relevant information. Where appropriate, this might include technology aids to assist with consistency and effectiveness, such as:

- Automated reminders to custodians.

- Information governance tools that check volumes of stored information in preserved locations.
- Audits of technology settings that effectuate legal holds.

Indeed, automated procedures can help organizations handle legal holds consistently and offer greater protection against accidental disclosures of personal data.

Additionally, when implementing a legal hold, an organization should be aware that foreign nationals and employees working in other jurisdictions might use different technologies to communicate, create, and store information than those used by their US colleagues. For example, Europeans frequently use the mobile app WhatsApp to communicate instead of more expensive text messaging. Practitioners should consider these geographic preferences when implementing a legal hold and discuss with IT professionals the best means of preserving this information (see [IT Practices](#)).

### Confirming Receipt

After distributing the legal hold notice, the organization must take affirmative steps to ensure that the recipients comply with it ([915 Broadway Assocs. LLC v. Paul, Hastings, Janofsky & Walker, LLP](#), 2012 WL 593075, at \*9 (Sup. Ct. N.Y. Cty. Feb. 16, 2012); see also [GN Netcom v. Plantronics](#), 2016 WL 3792833, at \*6-8 (D. Del. Jul. 12, 2016)). Often, an organization memorializes its process for confirming that each custodian received the legal hold notice and understands how to respond to the hold and preserve the relevant information. Organizations accomplish this confirmation process by, for example:

- Collecting read receipts, if the organization distributes the notice by email.
- Conducting personal interviews of the key custodians or all custodians, depending on the stakes at issue in the underlying matter, either in-person or by telephone or email. Generally, auto-generated template email questionnaires are sufficient, but individualized conversations may be more appropriate in especially complicated or high-exposure matters.

### Handling Redundancy

For many multinational organizations, documents and ESI reside in multiple locations and jurisdictions and with multiple custodians. A legal hold may require preservation of either only one copy of unique information or multiple copies of a document (see [Orbit One Commc'ns, Inc. v. Numerex Corp.](#), 271 F.R.D. 429, 436 (S.D.N.Y. 2010) ("a party is well-advised to retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches") (internal quotations omitted)).

Although a response to regulatory requests or discovery demands may not require multiple copies of the same information, usually the best practice is to provide for legal holds that are essentially redundant despite the duplication. Capturing redundant information in a legal hold notice:

- Ensures that the organization adopts a custodian-by-custodian approach.

- Informs individuals that their information is subject to a hold.
- Mitigates any potential issues raised by automatic deletion mechanisms.
- Enables the organization to adequately respond to specific regulatory requests or litigation discovery demands inquiring about whether a particular individual had (or has) access to a particular document, even if these requests are rare in practice.

Data protection concerns likely outweigh the advantages of preserving duplicative materials. Therefore, organizations should consider whether it is necessary to preserve EU versions in addition to US copies.

### **Modifying a Legal Hold**

An organization, and typically the legal department, has a continuing responsibility to expand or narrow the scope of the legal hold as circumstances warrant. The responsible legal representative should document the justification for any changes or updates to the legal hold including, most importantly, any decisions to lift the legal hold.

If the organization determines that it can release a specific legal hold, it must consider other legal holds within the organization that may require the ongoing preservation of information before releasing the hold.

For a sample legal hold lift notice that in-house counsel can use to notify legal hold recipients that the matter has concluded and the legal hold is no longer in effect, see [Standard Document, Litigation Hold Lift Notice](#).

### **Reviewing Relevant Organizational Policies**

Practitioners planning a cross-border legal hold should consult personnel responsible for organizational policies concerning:

- Information governance and record retention (see [Information Governance and Record Retention](#)).
- Bring Your Own Device (BYOD) programs (see [BYOD Programs](#)).
- Human resources (HR) functions (see [HR Policies and Practices](#)).
- IT practices (see [IT Practices](#)).

### **Information Governance and Record Retention**

The legal department should direct discussions on multinational information governance issues associated with legal holds with:

- Records managers, who maintain an organization's record retention schedules and related retention periods in any countries where relevant information may be located.
- IT professionals, who maintain the machines affected by the legal holds.
- Information security professionals, who maintain the controls associated with information about a legal hold.

Discussions with records managers often are critical because they provide guidance on how the organization typically keeps information. These professionals can identify certain types of information that, due to regular retention practices, may not require a specific legal hold collection practice because the organization retains them in the ordinary course of business (in which case, counsel should confirm that the operative technology is working properly). Conversely, these professionals can also identify information that is near its expiration date (or the date on which it would be automatically deleted under existing organizational retention plans), which might need extra care and structure to help prevent its deletion.

For an overview of the components of an effective information governance program and common information governance projects, see [Practice Note, Information Governance: Establishing a Program and Executing Initial Projects](#).

For a collection of resources in-house and outside counsel can use to manage an organization's records and other data, including sample record retention schedules, see [Records Management Toolkit](#).

### **BYOD Programs**

An organization that permits or requires employees to use their own devices should contemplate steps it might need to take to collect information from an employee's personal device. While organizations should respect employee privacy rights during preservation and collection activities, US and non-US BYOD policies should delineate the organization's right to access a device and the data stored on the device both for work-related activities and legal hold purposes.

For a sample BYOD policy that employers can implement to allow employees to use their own smartphones, tablets, or other mobile devices for work, see [Standard Document, Bring Your Own Device to Work \(BYOD\) Policy](#).

### **HR Policies and Practices**

HR involvement in legal hold practices can begin as early as when an employee first joins an organization and consents to its organizational policies. However, as discussed above, EU law has traditionally looked skeptically at whether employees can truly give consent when their job is on the line. Therefore, organizations should consider, as part of their HR onboarding processes, informing non-US employees who may be involved in US discovery issues about US-style legal holds and how they may be subject to them. However, this extra step is likely impractical for corporations whose non-US employees are rarely involved in US discovery issues.



Additionally, an organization should make the HR function aware of existing legal holds or otherwise coordinate procedures for departing employees who are on legal hold. HR might know before the legal department about the departure of an employee on legal hold, which may impact how the organization handles:

- The employee's exit interview.
- The transfer of:
  - physical documents in the departing employee's possession; or
  - data on the departing employee's personal or work-issued devices.

### IT Practices

An organization must keep the IT function apprised of existing legal holds affecting US and non-US information and involved in their implementation. Like the HR function, IT might know before the legal department that an employee on legal hold is departing, which might impact the transfer and preservation of any work-issued devices and data contained on those devices.

Additionally, IT is likely to know about instances when an individual on legal hold:

- Possesses a device that failed and needs replacement.
- Leaves the organization, making a departing employee's devices susceptible to being "wiped" and repurposed.
- Might be affected by an organization-wide rollout of new technologies or devices.

Organizations typically memorialize these practices in formal IT policies. For example, IT may have a checklist to consult before repurposing a device or computer. Having IT personnel confirm whether an employee was on hold when departing (and before wiping employee devices) is a best practice to ensure the preservation of potentially relevant data.

### Best Practices for Cross-Border Legal Holds

Given the potential conflicts of laws, practitioners planning to implement a legal hold abroad should be mindful in limiting the scope of the data sources subject to the hold. Some best practices organizations can follow to achieve this include:

- Limiting the scope of preservation to only data that is relevant, proportionate, and necessary to support claims or defenses by, for example:

- carefully identifying key custodians;
- interviewing key individuals;
- including questionnaires as part of the legal hold process; and
- asking custodians which sources of relevant information might also implicate personal data and sensitive personal data.

(For more information, see [Identifying Relevant Information and the Scope of Preservation](#).)

- Documenting the steps the organization took to determine how to appropriately limit the scope of preservation by, for example:
  - memorializing the information provided by key individuals that supported the organization's decisions on the scope of preservation;
  - preserving completed questionnaires included with the legal hold notices; and
  - recording the sources of relevant information that might also implicate personal data or sensitive personal data.

(For more information, see [Drafting a Legal Hold Notice](#).)

- Preserving in place in the original data location when possible and confirming with IT professionals the effectiveness of those preservation steps.
- Limiting out-of-country data preservation efforts and, if necessary, preserving data only in countries that are "white listed" or deemed to have adequate data protection safeguards. There may be additional considerations in cases where in-country preservation is not available under US law, for example, if the discovery of relevant information located abroad violates US EAR rules, triggers ITAR restrictions, or implicates OFAC sanctions (see [Transferring Personal Data](#)).
- Memorializing the steps of any specific document preservation process or procedure used in cases of regulatory scrutiny associated with the legal hold process, including:
  - monitoring any vendor involvement, including their protection of personal information, and encrypting personal information when possible (for more information, see [E-Discovery Project Management Checklist](#));
  - detailing local or regional counsel involvement and related advice;
  - maintaining records of legal hold implementation and release timing; and

- monitoring chain of custody documentation (for more information, see [Standard Document, Data Collection: Chain of Custody for Digital Media](#)).
- Considering a tiered or phased discovery process, in which an organization preserves US-based custodial data immediately and international custodial data after identifying the specific data needed. This approach could be limited by retention schedules of the relevant data.

Additionally, multinational organizations should have information regarding their international operations and sources of information (see [Data Maps](#)) so that they can readily determine where relevant information exists outside of the US.

An organization may also consider drafting country-specific legal hold procedures that separate legal holds by country and indicate that the organization might amend these non-US holds at a later time. Separating legal holds by country or jurisdiction enables an organization to communicate different expectations based on the approach taken in each respective jurisdiction. However, it may not be practical or necessary to implement country-specific holds in every matter.