

12

Multinational Aspects of SEC Investigations

*Edward T. Kang & Paul N. Monnin**

The SEC's enforcement program has increasingly involved multinational actors. These include foreign companies and their agents who are suspected of having engaged in securities law violations within the United States, along with domestic companies and their officers who are believed to have engaged in securities law violations outside the United States, but which nonetheless implicate U.S. jurisdiction. The SEC's investigation of these matters often involves complex issues of jurisdiction, privilege, privacy, and reliance on corporate actors, international securities regulators, and law enforcement agencies to conduct fact-gathering beyond the territorial reach of the United States.

* Daniel J. Felz of Austin & Bird LLP also served as an author of this chapter. He, Mr. Kang, and Mr. Monnin are partners at Alston & Bird LLP. Alston & Bird associates Leila Knox and Peter Cornick also contributed to this chapter.

This chapter provides an overview of multinational investigations and answers questions regarding the ways in which the SEC is able to obtain documents and to investigate across borders. In addition, it addresses some of the major pitfalls individuals and businesses face when responding to an SEC enforcement inquiry or performing an internal investigation that spans the globe.

Methods of Conducting Multinational Investigations	12-2
Privilege Considerations When Conducting Cross-Border Investigations.....	12-6
Document Production/Data Privacy Considerations	12-12
Global Coordination	12-35
Appendix 12A: Current Signatories of the IOSCO MOU	App. 12A-1

Methods of Conducting Multinational Investigations

Q 12.1 What is the SEC’s subpoena power in multinational investigations, at home and abroad?

By virtue of section 21(a) of the Exchange Act,¹ the SEC has broad and general power to “make such investigations as it deems necessary to determine whether any person has violated, is violating, or is about to violate” the federal securities laws. In domestic investigations, the SEC is given broad subpoena powers to command the “attendance of witnesses and the production of any such records . . . from any place in the United States or any State at any designated place of hearing.”²

Outside the United States, however, the SEC’s direct ability to compel production of evidence by subpoena is severely limited. The SEC does not have power to compel the production of documents or other evidence from persons who do not reside in and have no

jurisdictional ties to the United States.³ In addition, unlike the DOJ, the SEC is unable to issue *Bank of Nova Scotia* or PATRIOT Act subpoenas to obtain information or testimony of individuals located outside of the United States.⁴

Q 12.2 How do regulatory agencies typically gather evidence when conducting multinational investigations?

There are a number of tools available to the SEC when seeking to gather evidence abroad. Today, the most popular such vehicle is a Memorandum of Understanding (MOU). An MOU is a mutually beneficial agreement entered by two or more jurisdictions establishing a commitment to assist each other in the collection of evidence in jurisdictions beyond each party's regulatory reach. An MOU sets forth the terms pursuant to which evidence may be shared between its signatories, thereby facilitating multinational cooperation with compliance and enforcement efforts. Because MOUs are typically executed between regulatory agencies (as opposed to diplomatic entities), they can often be used to gather evidence for civil, as well as criminal, investigations. The SEC is party to over thirty MOUs with its foreign counterparts.⁵

In 2002, the International Organization of Securities Commissions (IOSCO) issued the "IOSCO MOU," which established guidelines for multinational information gathering.⁶ The IOSCO MOU allows its signatories to (1) obtain materials relating to transactions in both brokerage and bank accounts, as well as information pertaining to the corresponding account holders and beneficial owners; (2) compel testimony and/or official statements from individuals; and (3) share regulatory agency files across borders.⁷ The IOSCO MOU further provides that the parties that collect such information may use it directly in both administrative and civil venues, as well as provide it to criminal authorities, such as the DOJ.⁸ The IOSCO MOU has over 125 signatories, making it a significant and useful document in facilitating and expediting international investigations.⁹

In May 2019, the SEC and CFTC became signatories to the "Enhanced MOU," which expanded the powers available under the IOSCO MOU.¹⁰ The Enhanced MOU allows signatories to obtain and share materials

related to audits, to compel the physical attendance of individuals for testimony, and to freeze assets where possible, as well as to share internet service provider and telephone records.¹¹ As of the end of 2022, there were twenty-two signatories to the Enhanced MOU.¹²

Notably, the terms of MOUs often restrict a regulatory agency from withholding requested information on grounds of bank secrecy or other privacy laws. As such, caution should be exercised when relying on an MOU, as its terms may reflect or incorporate the policy concerns and regulatory schemes of a foreign jurisdiction—such as data privacy laws—that contradict or are incompatible with U.S. law and practices.

Q 12.3 What other types of international agreements assist regulatory agencies in gathering evidence in multinational investigations?

Mutual Legal Assistance Treaties (MLATs) are also commonly used to obtain evidence located in foreign countries. MLATs permit the Department of Justice (DOJ) and its foreign counterparts to request each other's assistance in gathering evidence in criminal investigations.

Traditionally, MLATs included a dual criminality requirement, which required the conduct under investigation to constitute criminal activity under the laws of both the country requesting assistance and the country providing it.¹³ In a recent trend, however, MLATs have been read to permit criminal authorities to obtain and share information obtained pursuant to an MLAT request with other regulatory enforcement authorities—including the SEC—irrespective of whether the “dual criminality” requirement is satisfied, so long as a criminal prosecution or referral is contemplated by the investigation.¹⁴

In addition to MLATs, the United States is a signatory to the Hague Convention on the Taking of Evidence Abroad (the “Hague Evidence Convention”).¹⁵ The Hague Evidence Convention is designed to facilitate cooperation between judicial authorities of different jurisdictions to enable cross-border evidence collection by bypassing traditional consular and diplomatic channels. For securities investigations, the Hague Evidence Convention is likely to play a marginal role because

(1) it applies only to “civil or commercial matters,” not to administrative investigations;¹⁶ and (2) evidence requests must be issued by a court, implying the need for judicial proceedings to have been initiated.¹⁷

Q 12.4 How can a regulatory agency obtain evidence in the absence of a treaty?

In the absence of an MOU or a treaty, the primary means for obtaining evidence in a foreign country is a letter rogatory, or a formal request by a domestic court to a foreign court, which requests that the foreign court compel a person within its jurisdiction to provide testimony or produce documents.¹⁸ U.S. statutes and case law permit U.S. federal courts to issue letters rogatory.¹⁹

Once a letter rogatory is issued, it is often transmitted directly by the requesting court to the receiving court.²⁰ Some governments, however, require that the letter rogatory pass through a diplomatic channel, such as the ministry of foreign affairs of the country where the evidence resides.²¹ Other foreign governments permit a letter rogatory to be transmitted by counsel admitted in the foreign court.²²

Foreign courts are under no obligation to execute letters rogatory,²³ and those that do may place restrictions on the scope of the evidence requested.²⁴ Furthermore, obtaining discovery pursuant to a letter rogatory will normally involve following the procedures of the foreign court, which may diminish the usefulness of the evidence obtained.²⁵

Obtaining evidence through letters rogatory may pose other issues specific to regulators. First, letters rogatory can generally only be used for gathering evidence in the course of litigation and likely will not have much utility in the investigative stage of a case.²⁶ For example, a letter rogatory may only be issued in connection with a judicial proceeding, and may not be available to assist a regulator where only an agency investigation or internal administrative proceeding is pending.²⁷ In addition, a letter rogatory generally cannot supersede foreign bank secrecy laws, and bank information is often essential to regulatory investigations.²⁸ It is also important to consider that the issuance of a letter rogatory is often a time-consuming process that can take up to a year or more to complete.²⁹

Privilege Considerations When Conducting Cross-Border Investigations

Q 12.5 What protection do privileged communications receive in cross-border investigations?

While the concept of attorney-client privilege is embedded in U.S. common law, many civil law jurisdictions across the world do not recognize this privilege. For example, in China, attorney-client communications are within the scope of a lawyer's duty to maintain client information confidentiality, but lawyers could be compelled to disclose information that is required by law or a court order. In South Korea, the law does not recognize the attorney-client privilege, but relies on lawyers' ethical obligations of confidentiality. There may be "testimonial immunity" that may protect attorneys from being compelled to reveal client secrets, but clients cannot invoke this immunity.

The "joint defense" or "common interest" privilege—which "serves to protect the confidentiality of communications passing from one party to the attorney for another party where a joint defense effort or strategy has been decided upon and undertaken by the parties and their respective counsel"³⁰—may be asserted in cross-border investigations that commonly focus on similarly situated employees or entities. Other common law countries, like the U.K., broadly interpret the common interest privilege, as well as the attorney-client privilege. Countries outside the Anglo-American legal tradition, however, including countries with civil law traditions, often take a narrower view of these ancillary or derivative privilege claims. For example, some civil law jurisdictions within the EU would refuse to extend the privilege to communications between a corporate employee and in-house counsel—a significant issue for corporations that face investigation in those countries.³¹

In light of the varied treatment that attorney-client communications receive globally, attorneys should familiarize themselves with the privilege rules of any relevant foreign jurisdiction. Practitioners should also consult with and, if necessary, retain local lawyers in the foreign jurisdiction to navigate privilege issues safely.

Q 12.6 When does U.S. privilege law apply to a foreign communication involving an attorney admitted or located in a foreign jurisdiction?

To determine whether to apply U.S. privilege law to a communication with an attorney admitted or located in a foreign jurisdiction, many U.S. federal courts have adopted the “touch base” approach. Under this conflict-of-law “contacts” analysis, a court applies the law of the foreign jurisdiction if the foreign jurisdiction “has the most compelling or predominant interest in whether the communications should remain confidential,” unless the court finds the law of the foreign jurisdiction contrary to public policy.³² As articulated by courts in the Second Circuit, “[t]he jurisdiction with the predominant interest is either the place where the allegedly privileged relationship was entered into or the place in which that relationship was centered at the time the communication was sent.”³³ As a rule, “[c]ommunications concerning legal proceedings in the United States or advice regarding United States law are typically governed by United States privilege law, while communications relating to foreign legal proceedings or foreign law are generally governed by foreign privilege law.”³⁴

Many EU Member States refuse to extend the attorney-client privilege to communications with in-house counsel, a conflict with the law in the United States. Therefore, whether a U.S. court would recognize a privilege claim for communications with foreign in-house counsel depends on the identity of the participants, where the communications occurred, and whether they were directed to the merits of a U.S. legal proceeding.



CASE STUDY: *Claims of Privilege over Communications with Foreign In-House Counsel*

In the *AstraZeneca LP v. Breath Ltd.* case, a court in the District of New Jersey ordered a Swedish company to produce correspondence between the company's in-house attorneys and employees, all of whom worked in Sweden.³⁵ The court reached this decision after it found the communications did not "touch" the United States, because the documents at issue neither involved U.S. proceedings nor communications with U.S. attorneys.³⁶ The court noted that, under Swedish law, the legal bar does not include in-house counsel; therefore, the communications with in-house counsel in Sweden were not privileged under Swedish law and could not be withheld.³⁷

In *Veleron Holding, B.V. v. BNP Paribas SA*, the Southern District of New York was confronted with an argument by the parties that the privilege law of four different countries applied—Russian, Dutch, British, and Canadian.³⁸ The court found that "the touch base analysis" favored application of Russian or Dutch attorney-privilege law as the communications at issue occurred in those countries.³⁹ The parties did not dispute that "Russian law does not recognize attorney-client privilege or work product immunity for communications between or work product by 1) in-house counsel; or 2) 'outside' counsel who are not licensed 'advocates' registered with the Russian Ministry of Justice."⁴⁰ The Netherlands does not recognize any privilege between a client and an unlicensed lawyer.⁴¹ Because the plaintiff did not provide information establishing that the Russian attorneys were registered with the Ministry of Justice nor any information that the Dutch attorneys were licensed, the court held that the plaintiff had not met its burden of demonstrating that the communications were protected under either nation's privilege law.⁴²

A court in the District of Delaware reached a different result in *Renfield Corp. v. E. Remy Martin & Co.*⁴³ There, it was U.S. employees who sought legal advice from in-house counsel

located in France, which, under its law, does not recognize communications with in-house counsel as privileged.⁴⁴ Because the employees seeking legal advice were based in the United States, the court found the United States had “the most significant relationship with the communication.”⁴⁵ Therefore, the court applied U.S. law and refused to compel production of the communications with in-house counsel.⁴⁶

Q 12.7 Would courts in the EU apply the attorney-client privilege to communications between a U.S. attorney and a client in the EU?

With respect to communications between a U.S. attorney and a client in the EU, the scope of the privilege from the perspective of a court within the EU would depend on the nature of the action. For an action brought in the national court of a Member State or an enforcement action initiated by the authorities of a Member State, the privilege rules of the relevant Member State would apply. On the other hand, if the European Commission initiated the enforcement action, then the privilege law of the EU applies. To understand the distinction, one can think of the EU privilege law as akin to the federal common law on privileges, which applies to federal actions. Compared to courts in the United States, courts in the EU take a narrow view of the attorney-client privilege, and a U.S. attorney who seeks to offer legal advice to a client in the EU must guard against inadvertent disclosure or waiver of the privilege.

The attorney-client privilege under EU law, called the legal professional privilege, has some significant distinctions from U.S. privilege law⁴⁷ and stems, in large part, from two key decisions of the European Court of Justice. In the first decision, *AM & S Europe Limited v. Commission of the European Communities*, the court established legal professional privilege under EU law.⁴⁸ As defined by the court, the privilege applies to communications that satisfy two elements: (1) the communication must be “made for the purposes . . . of the client’s rights of defen[s]e”; and (2) the communication must “emanate

from independent lawyers, that is to say, lawyers who are not bound to the client by a relationship of employment.”⁴⁹ The second element excludes in-house lawyers from the privilege.

In addition to the exclusion for in-house counsel, the court found that the privilege applied only to communications between a client and a “lawyer entitled to practi[c]e his profession in one of the Member States” and would not extend beyond those limits.⁵⁰

In the second key decision, *Akzo Nobel Chemicals Ltd. & Akros Chemicals Ltd. v. European Commission*, the European Court of Justice affirmed the holding in *AM & S* and confirmed that communications between in-house counsel and their corporate clients fall outside the scope of the attorney-client privilege.⁵¹ Specifically, the court found that emails between corporate executives and their in-house counsel would not receive the benefit of the attorney-client privilege.⁵² The European Commission had seized the emails during a “dawn raid,” which permits the European Commission to enter a business or residential premises to seize documents located on-site and to question the occupants.⁵³

In *Akzo Nobel*, the court did not revisit whether the privilege would extend to communications with attorneys not admitted in the EU. Based on the foregoing authority; however, a U.S. attorney should assume that, by virtue of his/her status as a foreign lawyer, an EU court would find that his or her communications with a client in the EU fall outside EU privilege law. This is true even if the U.S. attorney offers the client advice on U.S. law. Therefore, a U.S. attorney should confer with and channel all legal advice through the client’s external counsel in the EU.

Q 12.8 Would a U.S. court consider the privilege waived for documents produced in response to a request from the European Commission or from some other foreign enforcement agency?

Under U.S. law, “involuntary or compelled disclosure does not give rise to a waiver” of the attorney-client privilege.⁵⁴ Therefore, the question of whether a U.S. court would consider the privilege waived for

documents disclosed to the European Commission or to some other foreign enforcement agency depends on whether the court finds the disclosure voluntary or involuntary. This again raises the issue of whether a privilege is even recognized under local law. In the absence of a subpoena or judicially compelled disclosure, it becomes less clear whether a court would find a disclosure to a foreign enforcement agency voluntary or involuntary.⁵⁵

In the EU and many of its Member States, a dawn raid does not require a warrant or any other form of judicial intervention. Because a dawn raid results in the disclosure of potentially privileged documents that was not judicially compelled, a court would likely look at the steps taken to contest the disclosure, as well as the consequences for a failure to comply, in order to determine whether the disclosure was voluntary.⁵⁶ For that reason, a party should, before it provides documents to the European Commission, document its attempts to contest the disclosure and produce the documents only upon receipt of a clear indication that the European Commission would impose penalties or sanctions for a failure to comply.

Where the disclosing party did not have an opportunity to contest the disclosure, a court would likely find the disclosure involuntary. For example, in *In re Parmalat*, the plaintiff argued that a bank waived the attorney-client privilege with respect to documents the Italian authorities seized during a dawn raid and later disseminated to private plaintiffs.⁵⁷ The bank argued that the authorities seized the documents without the bank's consent and, therefore, the seizure could not operate as a waiver of the attorney-client privilege.⁵⁸ The court agreed and found that the bank was never provided with an opportunity to challenge seizure of the documents.⁵⁹ After the court found the disclosure to the Italian authorities involuntary, and the privilege preserved, the court next examined whether the bank took reasonable steps to preserve the confidentiality of the documents at issue, after the seizure by the authorities.⁶⁰ The court found the bank took steps "reasonably designed" to preserve the privilege when it asserted its privilege claim promptly after it learned the plaintiff planned to use the documents in depositions.⁶¹

Document Production/Data Privacy Considerations

Q 12.9 What is data privacy and why is it important when undertaking cross-border investigations?

In recent years, many countries have passed data privacy laws to protect their citizens' personal data and to regulate how individuals and businesses collect, process, use, store, disseminate and disclose personal data. These countries include, but are not limited to, members of the European Economic Area,⁶² Japan,⁶³ China,⁶⁴ Brazil,⁶⁵ Russia,⁶⁶ India,⁶⁷ Canada,⁶⁸ Switzerland,⁶⁹ the United Arab Emirates,⁷⁰ Mexico,⁷¹ and Taiwan.⁷²

Accordingly, before document collection efforts begin during a cross-border investigation, it is vital to understand the applicable data privacy rules and regulations of each country involved, as well as any potential differences or conflicts between those laws. This is particularly important as many countries have instituted civil and sometimes even criminal liability for violation of their data privacy laws.

Q 12.10 Does the United States have a data privacy law?

Notably, the United States does not have a universal data privacy law similar to the laws enacted by many of the countries cited above. Instead, the United States has a variety of laws and regulations, at the state and federal level, as well as non-binding guidelines from government agencies that were developed over a number of years. For purposes of cross-border investigations, one important U.S. regulation to consider is SEC Regulation S-P.

In 2000, the SEC adopted and implemented Regulation S-P, 17 C.F.R. § 248, which is comprised of privacy rules promulgated under section 504 of the Gramm-Leach-Bliley Act.⁷³ As discussed in the release of the SEC's final rule, section 504 of the Gramm-Leach-Bliley Act required the SEC and other federal agencies "to adopt rules implementing notice requirements and restrictions on a financial institution's ability to disclose nonpublic personal information about

consumers.”⁷⁴ Furthermore, the Act required financial institutions to provide their customers with notice of their privacy policies and practices, and prevented them from disclosing non-public personal information about a consumer to third parties without notification to the consumer.⁷⁵

Q 12.11 What kind of liability can an individual face for violating Regulation S-P?

The SEC has charged and assessed penalties against firms for violation of Regulation S-P. For example, in 2008, the SEC fined NEXT Financial Group, Inc. \$125,000 for encouraging brokers it recruited to transfer, from the brokers’ former employers, customer account information, including Social Security numbers, net worth and account numbers.⁷⁶ The SEC found that the brokers who left their firms and joined NEXT should have provided notice to their customers and obtained permission from them before transferring their private information to NEXT.⁷⁷ Likewise, in 2009, the SEC fined Woodbury Financial Services, Inc. for violating Regulation S-P by allowing its recruits to bring personal customer information to Woodbury, and also allowing employees, who were leaving Woodbury, to take private customer information to other firms.⁷⁸ In 2016, Morgan Stanley agreed to pay a \$1 million settlement for failing “to adopt written policies and procedures reasonably designed to protect customer data.”⁷⁹ As a result of that failure, between 2011 and 2014, “a then-employee impermissibly accessed and transferred the data regarding approximately 730,000 accounts to his personal server, which was ultimately hacked by third parties.”⁸⁰

The SEC also continues to charge individuals directly with violations of Regulation S-P. For example, in 2011, the SEC fined three executives from GunnAllen Financial Inc., including its chief compliance officer, a total of \$55,000 for transferring personal information of more than 16,000 of their customers to another firm without providing notification to the customers.⁸¹ This was the first time the SEC ever charged and assessed penalties against individuals solely for violating Regulation S-P.⁸² More recently, in 2016, the SEC settled with a brokerage firm and two of its principals for alleged violations of Rule 30(a) of Regulation S-P for using non-firm email addresses to receive over 4,000 faxes from customers and third parties that

routinely included sensitive customer information.⁸³ The broker-dealer was fined \$100,000 and the two principals were fined \$25,000 each.⁸⁴

Q 12.12 What liability do parties face in connection with violations of data privacy regulations of foreign jurisdictions?

Cross-border discovery is a component of many U.S. investigations, and foreign entities with U.S. affiliates or subsidiaries often face significant pressure to produce documents or other information to U.S. regulators. U.S. regulators, as well as private litigants, must consider the data privacy laws and regulations of the foreign countries in which the requested information is located, and must weigh the penalties associated with failing to comply with these laws against the penalties for failing to comply with U.S. discovery requests, should a conflict between the two arise.

The following sections provide guidance on the data privacy laws of the European Union, the United Kingdom and Russia.

Q 12.13 In securities enforcement actions, will European Union privacy law apply to production of documents that are located in the EU?

The production of documents, records, and/or ESI located in the EU will involve the processing of personal data and result in the application of EU privacy law. As of May 25, 2018, the EU's General Data Protection Regulation (GDPR) sets forth a uniform statutory basis of privacy law throughout the EU.⁸⁵ The GDPR fully repeals and replaces the EU Data Protection Directive that existed prior to May 2018.⁸⁶ Together with local statutes passed by the EU Member States implementing certain GDPR provisions, the GDPR sets forth the privacy law with which organizations must comply when producing records from the EU.

One of the more notable differences between the GDPR and pre-GDPR EU privacy law is the level of fines that European privacy supervisory authorities can impose upon companies that commit privacy violations. The GDPR permits companies to be fined up to €20 million

or 4% of annual worldwide revenue, whichever is greater, for privacy violations.⁸⁷ Additionally, the GDPR permits individuals who have been affected by a privacy violation to bring suits to recover “non-material damages.”⁸⁸ Thus, one effect of the GDPR is to increase the risk profile associated with privacy violations, including privacy violations that occur in the course of responding to U.S. legal proceedings.

This section briefly (A) outlines why the GDPR generally will apply to document discovery activities affecting EU data, then (B) points out resulting legal issues that arise from EU privacy law in the context of document discovery.

Q 12.13.1 How does the GDPR apply to document production in securities enforcement actions?

The GDPR will apply to document production activities conducted within the EU because the typical stages of document discovery will qualify as GDPR-regulated processing of personal data. The GDPR governs the “processing” of “personal data” that relates to EU citizens. Both of these terms are defined broadly, such that the activities involved in conducting document discovery—preservation, collection, review, redaction, transfer to the United States, and production—will likely implicate the GDPR.

- “Personal data” is defined as any information that relates to an identified or identifiable natural person.⁸⁹ Personal data is not limited to information that would be considered “personally identifiable information” in the United States—such as name or social security number—but also includes any further information that can be reasonably associated with or linked to an EU individual. Furthermore, the definition of “personal data” does not distinguish between “public” versus “private” data, or “private” versus “business” data; if information can be associated with an individual, it is GDPR-regulated personal data. Examples of personal data potentially relevant to document discovery include work email address, job title, performance appraisals, document metadata, Internet protocol address (IP address), online browsing data, and company IT usage logs. Records containing such information will either constitute or contain personal data.

- “Processing” is defined broadly as “any operation or set of operations which is performed on personal data,” irrespective of whether performed “by automated means.”⁹⁰ Relevant to document production, the GDPR expressly provides that processing includes “storage,” “retrieval,” “disclosure by transmission, dissemination, or otherwise making available,” as well as “destruction.”⁹¹ Thus, each phase of production in response to a U.S. investigation is likely to involve “processing” as defined in the GDPR, including preservation, collection, review, and production.

As a result, counsel should presume that the ordinary course of document discovery will trigger application of the GDPR.

Q 12.13.2 What are key privacy issues associated with document discovery involving EU documents and records?

Given the risk of GDPR violations, companies should begin working with privacy counsel as soon as it becomes apparent that responses to U.S. government requests may require document production from the EU. The progressive globalization of the EU economy over the past decades has meant that ever more EU companies and regulators have experience with U.S. discovery. Often though, the local expectation will be that document production is not conducted as it is in the United States. It can be important to structure carefully the major aspects of how EU records will be collected, reviewed, transferred, and produced, often in conjunction with local EU stakeholders, prior to beginning the process.

The following represent some of the key legal issues that can be considered at the outset of any document production effort in response to U.S. government requests:

1. Purpose Limitation

The GDPR continues to codify a rule known in Europe as the “purpose limitation principle”: Companies may only process personal data for specific, defined purposes that have been disclosed to individuals at or prior to the time that data is collected.⁹² To use data for other purposes, either (a) the new uses must be deemed “compatible” under

EU law with the purposes that were initially disclosed to individuals,⁹³ or (b) the company must notify individuals of the new uses and obtain their consent.⁹⁴

Many companies use an employee privacy notice to put employees on notice that their personal data may be processed in connection with litigation. Still, there can be heightened sensitivity to document preservation and collection in EU jurisdictions, particularly to U.S.-style imaging of entire hard drives, servers, or email accounts. Counsel should be aware of what data processing purposes have been communicated to EU employees, and what employees' reasonable expectations may be. Going beyond such expectations is no longer merely a potential labor matter; it is now a possible GDPR violation.

2. Works Council Agreements

A number of European jurisdictions—including Belgium, France, and Germany—permit employees to enter into collective agreements with management.⁹⁵ One of the common types of such collective agreements is a “works council agreement,” concluded between the company’s “works council”—which is elected by and represents the company’s employees—and management.

Historically in Europe, works council agreements could contain special or customized data privacy rules for foreseeable intra-company data uses. It was not uncommon for works council agreements to contain procedures to be followed when the company needed to process and produce employee data to respond to litigation.

The GDPR continues to permit companies and labor to conclude works council agreements for this purpose.⁹⁶ Counsel should be aware of the potential for such agreements to exist, and of the potential for such agreements to contain rules or procedures that must be followed when conducting discovery in connection with U.S. investigations. The restrictions in such agreements can be significant. For example, works council agreements may require U.S. counsel to work with the local works council to create preservation, collection, review, and/or redaction procedures. Such agreements could also, for example, require document review to be conducted locally, or preclude U.S. counsel from directly interacting with EU document custodians without notice to, or approval of, the works council. Counsel

should be prepared to comply with works council agreements during discovery, as violating them could arguably constitute wrongful data processing in violation of the GDPR.

3. Lawful Basis Requirement

The GDPR codifies what EU law describes as the “lawfulness principle”—all processing of EU data must be based on one of six statutorily enumerated lawful processing bases:

- **Consent:** The affected individual has consented to the processing;⁹⁷
- **Contract:** Processing is necessary for the company to conclude or perform a contract with the individual affected by the processing;⁹⁸
- **Legal compliance:** Processing is necessary for the company to comply with obligations imposed on it by statutes of the EU or its Member States;⁹⁹
- **Vital Interest:** Processing is necessary to protect the “vital interests” of the individual affected by the processing (e.g., physical safety);¹⁰⁰
- **Public Interest:** Processing is necessary for the performance of tasks carried out “in the public interest” of the EU or a Member State, or “in the exercise of official authority”;¹⁰¹
- **Legitimate Interests:** Processing is necessary for the company to pursue its legitimate interests, and the countervailing privacy interests of the affected individuals do not outweigh the company’s interests.¹⁰²

Of the above, only “Consent” and “Legitimate Interests” are generally available to support the data processing conducted in connection with document production. Note, however, that there are key differences between each legal basis that can affect whether companies should rely on consent or their legitimate interests to support collection, review, and production:

- **Consent** must be given by a “clear affirmative action” of the affected individual that specifically authorizes the company to process the individual’s data for document discovery,¹⁰³

such as a signed consent declaration. Also, consent can be withdrawn at any time.¹⁰⁴ Thus, if a company obtains consent from an EU document custodian to collect, review, and produce his documents, the custodian can potentially revoke his consent, in whole or in part, at any time during the U.S. proceedings. Such a revocation may preclude the company from relying on or producing certain records relating to that custodian. Still, European companies or local works councils may expect consents to be obtained from document custodians prior to collecting their ESI; U.S. counsel should be ready to address the issue.

- Legitimate interests permit the company to rely on its own legitimate interest in exercising legal rights, or defending against legal claims, to conduct discovery. Thus, no written declaration from document custodians or other employees would be strictly required. Still, several considerations remain:
 - In practice, some companies at times consider providing a courtesy notice (without a consent declaration) to custodians if they believe it necessary to document that the custodian has been adequately informed that their personal data may be used for litigation or enforcement purposes and may be transferred out of the custodian's home jurisdiction for those purposes.
 - Even if no written declaration is requested from the individual custodian, or no courtesy notice is provided, it is generally advisable to document a "legitimate interests assessment" (LIA). The LIA documents an interest-balancing assessment by the company that (a) describes the company's legitimate interests in collecting, reviewing, and producing employee personal data for discovery and litigation purposes; (b) identifies the impacts on the privacy rights of affected individuals; (c) identifies measures the company will take in efforts to mitigate those impacts; and (d) determines whether, on balance, the company's interests outweigh the impacts on affected individuals' privacy rights, as the impacts have been mitigated by the company.

- Additionally, individuals retain a right to “object” to processing that a company bases on its legitimate interests, so long as the individual can show that the objection is based “on grounds relating to [the individual’s] particular situation.”¹⁰⁵ When such an objection is made, the company must evaluate the request and document its decision as to whether its interests in establishing, exercising, or defending the legal claims at issue are “compelling”; to the extent they are not, the processing must stop.¹⁰⁶ It is conceivable that custodian or other employee objections may preclude a company from relying on or producing certain records relating to the objecting individual, although such a determination would be made on an individual basis.

The decision as to which legal basis best fits a particular case should be made on a case-by-case basis. The company and its prior discovery practices, the number of EU custodians, the potential volume of EU production, and local regulatory expectations for obtaining consent may be relevant.

4. Transfer Restrictions

One key aspect of EU data protection law is its restrictions on transfers of personal data outside the EU. The GDPR’s general rule is that EU personal data cannot be transferred outside the EU. Any such transfers must be based on a statutorily recognized basis for transfer.¹⁰⁷ The EU’s transfer restrictions have clear relevance for companies’ ability to transfer relevant records to the United States as part of document collection, review, or production.

This section will note the major bases for data transfers and briefly note their potential applicability to U.S. document discovery in support of securities enforcement proceedings. Note, however, that even when relying on these mechanisms, European court decisions have begun to heighten the risks involved in transferring personal data to the United States; see section 5 below, on the ECJ’s *Schrems II* Decision, for a further analysis of emerging risks:

- Adequacy determination: Personal data can be freely transferred to any country the EU Commission has formally

decided provides “adequate protection” for personal data.¹⁰⁸ As of January 2019, twelve countries have been deemed adequate;¹⁰⁹ the United States is not included. Instead, until 2020, the EU and the United States had reached a compromise solution: individual U.S. companies could be deemed to provide adequate protection for EU data if they registered with the U.S. Department of Commerce as self-certified participants in the EU-U.S. Privacy Shield Framework.¹¹⁰ However, in July 2020, the European Court of Justice held the Privacy Shield Framework to be invalid under EU law, and it is thus no longer available to support data transfers to the United States. And in any case, U.S. government recipients, such as the SEC or DOJ, cannot join the Privacy Shield Framework. As discussed below, the EU and U.S. are working on a new successor framework to the Privacy Shield, entitled the “Transatlantic Data Privacy Framework.” This framework, if adopted by the EU, is expected to enter into force in late 2023 or early 2024.

- **Standard Contractual Clauses:** Personal data can generally be transferred to recipients outside the EU if the EU company transferring the data, and the non-EU recipient of the data, have executed contractual clauses approved by the European Commission (the “Standard Contractual Clauses”).¹¹¹ It is not uncommon for corporate affiliates to execute the Standard Contractual Clauses amongst themselves, permitting intra-company data transfers. However, companies that receive data under the Standard Contractual Clauses are generally restricted from transferring the data to a new recipient, even if in some circumstances some may read the Clauses as supporting arguments that they contemplate permitting compelled disclosures to “law enforcement” agencies.¹¹² Standard Contractual Clauses are not generally executed with litigation opponents, and particularly not with adverse U.S. government parties.
- **Derogations:** When neither an “adequacy” determination nor the Standard Contractual Clauses are available, the GDPR permits companies to rely on statutory “derogations” from

the EU's general data-transfers prohibition to transfer personal data outside the EU.¹¹³ Potentially relevant derogations include:

- **Consent:** EU individuals can consent to have their data transferred outside of the EU. Such consents must meet the GDPR's general requirements, i.e., they must be given via a "clear affirmative action" and be withdrawable at will.¹¹⁴ Further, prior to giving consent to transfers data to another country, EU individuals must be informed "of the possible risks of such transfers" due to the fact that the non-EU country does not offer "adequate protection," and no Standard Contractual Clauses are in place.¹¹⁵ In practice, consents may, and sometimes do, serve as both the legal basis for discovery-related data processing as well as the basis for transferring an individual's data outside of the EU.
- **Transfers for litigation purposes:** The GDPR permits transfers outside the EU when "the transfer is necessary for the establishment, exercise or defense of legal claims."¹¹⁶ Note that this derogation is not a blanket authorization to transfer data outside the EU in connection with litigation, but instead an authorization to transfer such data as is "necessary" to establish, exercise, or defend against specific claims or defenses. As a derogation from a general prohibition on transfer, the amount of data deemed "necessary" for U.S. litigation will likely be interpreted narrowly by EU regulators. Thus, even when relying on this derogation to transfer EU data to the United States in connection with U.S. document discovery, companies should consider working with counsel to structure collection, review, transfer, and production such that the data ultimately transferred to the United States can be defended as "necessary" in light of the claims and defenses asserted in the litigation.
- **One-time transfer for compelling interests.** If no other statutory basis for transferring data to the U.S. is available, companies can nonetheless transfer data to the

U.S. if (a) the transfer is not repetitive; (b) the transfer concerns only a limited number of individuals; (c) the transfer is necessary for the company to pursue compelling legitimate interests which are not overridden by affected individuals' privacy interests; (d) the controller has conducted a written assessment of all the circumstances surrounding the transfer and has provided suitable privacy safeguards; (e) the company specifically notifies affected individuals about the transfer; and (f) the company notifies the local privacy supervisory authority of the transfer.¹¹⁷ Transfers in the discovery context are theoretically possible under this derogation, but given the need to involve privacy regulators, may remain seldom.

5. Additional Transfer Risks under the European Court of Justice's *Schrems II* Decision

On July 16, 2020, the European Court of Justice (ECJ) introduced further considerations for EU-to-U.S. data transfers via its "*Schrems II*" decision.¹¹⁸ This case arose from a complaint raised by Maximilian Schrems, an Austrian privacy activist, against Facebook's transferring of EU user data to the United States. Mr. Schrems alleged that personal data subject to such transfers is not adequately protected in the United States because it could be covertly obtained by U.S. intelligence agencies under broad authorities, and because he allegedly had no effective judicial redress with which to challenge such practices.

The ECJ treated the *Schrems* case as an opportunity to decide the more general question of whether transfers of EU data to the United States remain lawful under EU law, and if so, under what conditions transfers can be considered legal. The ECJ held that the United States does not offer adequate protection for European personal data because (a) certain authorities under which U.S. intelligence agencies may collect data—particularly section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12,333—are overbroad and not proportionate, and (b) U.S. law does not provide EU citizens with effective judicial remedies by which they can challenge how U.S. intelligence agencies collect and use their data.¹¹⁹

As a result, the ECJ held that the Privacy Shield Framework was invalid.¹²⁰ It further held that, if companies wish to use Standard Contractual Clauses to transfer EU data into the United States, they must first assess that the specific transfer(s) to be supported by the Standard Contractual Clauses will enjoy essential equivalent protections to what they would have had in the EU. If they will not, the transferring parties should put in place “additional measures” (which the ECJ did not specify) to protect the transfer, or the transfer should generally not occur.¹²¹ The ECJ thus made the Privacy Shield unavailable and the Standard Contractual Clauses potentially more challenging to rely on to support EU-to-U.S. transfers.

Still, the ECJ’s decision indicated that the derogations remain available to support transfers of data to non-EU countries, including the United States. This would mean that—as outlined above—companies can still obtain consent from EU citizens in order to transfer their data to the United States.¹²² It would further indicate that companies can transfer personal data to the United States to the extent “the transfer is necessary for the establishment, exercise or defense of legal claims.”¹²³

The EU and United States are working toward a new framework that would enable EU-to-U.S. data transfers without the need to implement the “supplementary measures” discussed above. The framework is entitled the Transatlantic Data Privacy Framework (TDPF). If adopted by the EU, TDPF would enable U.S. companies to be listed as “TDPF organizations” by self-certifying they will comply with the privacy principles set forth in the TDPF to the U.S. Department of Commerce. If they do so, DOC adds the company to the “TDPF List” as a “TDPF organization,” and the now TDPF-certified company may receive unrestricted transfers of EU data. Note, however, that in registering as a TDPF organization, the company voluntarily submits to the enforcement jurisdiction of the Federal Trade Commission in cases where the company fails to comply with TDPF privacy principles.

6. Special Transfer Rules in the U.K. and Switzerland for SEC Investigations

Though the *Schrems* case did not specifically address U.S. litigation or investigations, some European privacy authorities have disclosed frameworks for data transfers made specifically in the context of SEC investigations and proceedings. In September 2020, the U.K.’s

Information Commissioner's Office (UK ICO) published a letter to the SEC indicating the formal steps SEC registrants could take to enable transfers to the SEC in connection with books and records inspections and examination requests directed toward a broad swath of securities industry participants the SEC regulates, including investment advisers, investment companies, broker-dealers, credit rating agencies, transfer agents, clearing agencies, exchanges, and trading venues, as well as U.K. issuers listed in the U.S.¹²⁴ In June 2021, the Swiss Federal Data Protection and Information Commissioner ("Swiss DPC") released a similar framework for SEC registrants to be able to provide personal data in response to SEC examination and inspection requests, while maintaining compliance with Swiss data protection laws.¹²⁵

At a high level, both the Swiss DPC framework and the UK ICO recognize an overriding public interest in responding to SEC examination and inspection requests, notwithstanding the potential data protection challenges they may pose. However, there are some key differences:

- The UK ICO generally requires companies to document a determination that transfers to the U.S. in connection with an SEC investigation are lawful. This involves documenting determinations that (a) any SEC requests giving rise to the transfer are within the SEC's regulatory powers, (b) the SEC requests are not "large scale and systemic," and (c) transferring personal data to the U.S. for use in SEC proceedings would be in the "public interest."
- The Swiss DPC also requires companies to document their determination that transferring personal data to the U.S. in connection with an SEC investigation is lawful. However, the Swiss DPC framework envisions a broader scope of entities that may potentially transfer data to the U.S. for SEC investigations. These include not only SEC registrants like investment advisers, broker-dealers, clearing agencies, and transfer agents, but also "Swiss-based entities that are not registered with the SEC, including audit firms, in furtherance of examinations of SEC registrants or in other limited circumstances."¹²⁶ Additionally, the Swiss DPC requires companies to document a case-by-case risk assessment that confirms that contractual

obligations or public interests favoring the transfer outweigh the interests of impacted individuals.¹²⁷

In other countries, it remains unclear how the ECJ's *Schrems* decision will influence cross-border discovery practice, particularly in U.S. government investigations or in matters where the U.S. government is an adverse party. The decision's invalidation of the Privacy Shield and the restrictions it placed on Standard Contractual Clauses suggest increased skepticism towards cross-border transfers; still, the ECJ appears to have left investigation- and discovery-related derogations intact. However, the ECJ's judgment arose from its concerns about how certain U.S. government agencies handle personal data. Although the ECJ's decision specifically dealt with U.S. intelligence agencies, it may not yet be prudent to assume the judgment cannot be read as a basis for scrutinizing disclosures to other parts of the U.S. government. Further, both the ECJ and subsequent statements by European privacy regulators¹²⁸ have emphasized that the responsibility for protecting EU data after it is transferred to the United States rests on the parties who transfer it. At the same time, regulators have not affirmatively endorsed transfers to the United States on the basis of derogations, instead merely stating that guidelines on derogations are available and "must be applied on a case-by-case basis."¹²⁹

The foregoing points to potentially increased risk, or at least increased near-term uncertainty, for cross-border transfers in discovery contexts where the U.S. government or U.S. agencies may be an ultimate recipient of EU data. Companies would be well advised to coordinate closely with counsel at the beginning of discovery to assess the evolving risk environment and determine its impacts for the structuring of document collection, review, and production.

7. Additional Transfer Restrictions on Compelled Disclosures—Requirement for an MLAT?

Document production in securities enforcement actions is generally assumed to be compulsory, be it due to applicable procedural rules or the propounding of a subpoena. The compulsory nature of production arises from the fact that, if a company does not produce as requested by the government, the government can obtain an administrative or court order compelling the company to produce. Prior to the GDPR, European privacy law contained no rules expressly addressing

situations where production of records was compelled by a U.S. court or agency. Now, however, the GDPR contains a new provision that may—or may not—restrict transfers of personal data to the United States in compelled-production scenarios. Article 48 GDPR states:

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a [company] to transfer or disclose personal data may only be recognized or enforceable . . . if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the [EU] or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter [V of the GDPR on international transfers].

This provision is new to the GDPR, and its ambiguous language potentially gives rise to both strict and permissive interpretations. A strict interpretation would read an “MLAT requirement” into the GDPR, i.e., data cannot be transferred outside the EU in response to a non-EU request for evidence—such as a U.S. administrative subpoena—unless an MLAT is in place with the recipient state.¹³⁰ In contrast, a more permissive reading would view an MLAT as one of many available bases for transfers to satisfy a non-EU request for evidence. Such a reading would emphasize that Article 48 of the GDPR expressly states it is “without prejudice to other grounds for transfer” set forth in the GDPR, thus permitting companies to continue relying on any of the above-outlined bases for transferring data to the United States, irrespective of whether an MLAT is in place.

It is unclear how EU courts and regulators will interpret Article 48 of the GDPR. Within the U.S., the case of *United States v. Microsoft Corp.* resulted in discussion of whether Article 48 requires the United States to conclude MLATs with EU Member States for U.S. government agencies to compel production of data located within the EU.¹³¹ In *Microsoft*, the FBI issued a subpoena to obtain the content of emails of a Microsoft user that had been stored on a server located in Ireland. Microsoft refused to produce the emails, arguing that the FBI must use the MLAT in force between the United States and Ireland to obtain the emails. The case was never decided because it was mooted by passage of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act).¹³² Nonetheless, prior to being mooted, amicus briefs were filed

by EU stakeholders that evinced a diversity of opinion as to how Article 48 should be read. For example, the European Commission argued that Article 48 makes MLATs “the preferred option” for discovery-related transfers, but that other GDPR-recognized bases for transfers remain available to companies.¹³³ In contrast, French, German, Irish, and Polish industry associations suggested Article 48 should be read as establishing that “foreign demands for data are not recognizable in the EU unless domesticated through an MLAT or other agreed-upon framework.”¹³⁴

Regulatory expectations and jurisprudence relating to Article 48 are likely to evolve as the GDPR is applied to more cross-border proceedings. Developments in the EU may also respond to and/or anticipate the evolving law in the United States under the CLOUD Act. Further, new diplomatic channels for compelled production may arise. For example, the United States and United Kingdom have signed a CLOUD Act agreement under which each country’s law enforcement agencies can request electronic evidence directly from providers in the other country, without having to go through the standard MLAT process.¹³⁵ The United States is currently negotiating similar agreements with Australia and the European Union.¹³⁶ In light of the ambiguity surrounding Article 48 and the evolving environment for cross-border requests, companies should work with counsel to determine the potential risks of responding to U.S. demands for production, and to structure appropriately risk-adjusted procedures to collect, review, and transfer data in response to such demands.

8. Ancillary Issues in Cross-Border Investigations

Even when the above issues are managed, European privacy laws can create ancillary issues that may require attention during and following the discovery phase of an investigation or subsequent litigation. These include:

- *Sensitive Data*: European privacy laws contain heightened restrictions for collection and use of sensitive personal data, generally defined as (a) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; (b) biometric or genetic data; (c) data concerning health; (d) data concerning sex life or sexual orientation; (e) in some EU countries, government-issued social

insurance and/or national ID numbers; and (f) data relating to prior criminal convictions.¹³⁷ The general GDPR rule for sensitive data is that it cannot be collected, used, or disclosed without documented, opt-in consent. The GDPR does contain a carve-out that permits sensitive data to be processed without consent as is “necessary” for “the establishment, exercise, or defence of legal claims”¹³⁸—but this carve-out does *not* apply to records of prior criminal convictions, which may be relevant in SEC enforcement matters, and which may thus continue to require consent to collect and disclose. As stated above, such consent can be revoked by the relevant custodian at any time. This can potentially complicate the discovery process and may counsel for considering alternatives to production such as, e.g., mutually agreed redactions.

- *Subject Access Requests:* The GDPR grants individuals statutory rights of “access,” i.e., a general right to request from companies a copy of personal data that is held and processed. Since GDPR terminology describes these requests as “access” requests made by a “data subject,” they are often referred to as “subject access requests” or “SARs.” These rights are generally applicable and remain relevant in the investigations context. European individuals can potentially seek to obtain copies of records about them stored in investigation files, or other records that are created in connection with investigations—including records that were created as part of the investigation or otherwise in anticipation of litigation. European practice varies on the extent of production required in response to such subject access requests. Some jurisdictions—such as the U.K.—readily require companies to comply with access requests even when it seems clear that the requesting individual may use records that are produced against the company producing them. Other EU jurisdictions are more limited in the scope of production required. On the whole, the presence of these rights generally counsels for circumspection in record creation and retention in connection with investigations.
- *Storage Limitation:* The GDPR mandates that personal data be retained for “no longer than is necessary for the purposes for

which the personal data are processed.”¹³⁹ This is generally referred to as the GDPR’s “storage limitation” principle; in U.S. terms, it corresponds to the concept of limiting retention periods for investigation files and litigation-based records. Counsel should consider setting purge periods for investigation files following the conclusion of SEC proceedings.

Q 12.13.3 Do blocking statutes play a role in ensuring GDPR compliance in EU document discovery?

Lastly, independent of the GDPR, some European jurisdictions maintain blocking statutes prohibiting the production of evidence in response to U.S. evidence requests. Blocking statutes are discussed in detail in QQ 12.15 through 12.17. Blocking statutes generally are not considered privacy rules, but their scope of application may overlap with privacy restrictions, and their effects on discovery may be similar. Blocking statutes and privacy restrictions tend to be best addressed in tandem at early stages of discovery, so that appropriate responses to the competing demands of U.S. discovery and foreign statutory requirements can be structured.

Q 12.13.4 Do GDPR rules apply within the United Kingdom?

The U.K. voted to exit the EU in the U.K.’s 2016 Brexit referendum, and then officially exited the EU in 2019. However, the U.K. broadly retained the GDPR as part of the U.K.’s own domestic law, with the U.K.’s version of the GDPR commonly being referred to as the “U.K. GDPR.”¹⁴⁰ Generally speaking, the U.K. GDPR’s rules tend to mirror those of the EU’s GDPR, although it is worth noting that the U.K. GDPR is subject to interpretive guidance of the U.K.’s own Information Commissioner, which may at times differ from that of the EU privacy supervisors charged with interpreting the EU GDPR.

In general, the U.K. GDPR—like its EU counterpart—will require companies to address the (1) purpose limitation, (2) works council, (3) lawful basis, and (4) transfer restriction issues discussed in Q 12.13.2 above. In regard to transfers in the context of SEC investigations, the following guidance from the U.K. Information Commissioner may be helpful.

First, the U.K. Information Commissioner has published guidance specifically finding that statutory permissions to transfer data as is “necessary for the establishment, exercise or defence of legal claims”¹⁴¹ applies to claims arising in “administrative or regulatory procedures (e.g., to defend an investigation (or potential investigation)).”¹⁴²

Second, as discussed in more detail in response to Q 12.13.2 above, the U.K. Information Commissioner published a letter to the SEC indicating the formal steps SEC registrants could take to enable data transfers to the SEC in connection with books and records inspections and examination requests.¹⁴³ This potentially enables a more structured and documented approach to data transfers from the U.K. to the U.S., including directly to the SEC, in connection with SEC investigations.

Q 12.14 How does Russian privacy law apply to document production in connection with securities enforcement actions?

Russian law similarly regulates and protects personally identifiable information (PII) under a number of laws and regulations, including:

- the Federal Law on Personal Data of 27 July 2006 No. 152-FZ (as amended), (the “PD Law”), which regulates the processing of PII;
- the Federal Law on Information, Information Technologies and the Protection of Information of 27 July 2006 No. 149-FZ (as amended), which regulates the searching, receipt, transfer, production and distribution of PII;
- the Labor Code of the Russian Federation of 30 December 2001 No. 197-FZ, which regulates the personal data of employees and the employers’ corresponding obligations relating thereto;
- regulations of Russian authorities in the data protection sphere; and
- decisions of the Russian government relating to personal data.

Unlike U.K. law, Russian law does not distinguish between the data controller and the data processor, and instead applies equally to all

“data operators” that organize or carry out the processing of personal data and records, either manually or electronically.¹⁴⁴ The processing of personal data for the purpose of promoting goods, work, or services in the market is allowed only if the prior consent of the person referenced in the personal data (the “data subject”) has been obtained or if the data falls within certain exceptions.¹⁴⁵ Examples of data falling within these “exceptions” include data that was previously made publicly available by or under the instruction of the data subject; data that is processed for the protection of the life, health or other legitimate interests of the data subject; and data that is processed in accordance with an international treaty or pursuant to Russian law.¹⁴⁶

Under Article 22 of the PD Law, PII may only be processed by a data operator upon prior written notification of the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor)—the authority that is authorized to protect the rights of personal data subjects—unless certain exemptions apply.¹⁴⁷ A data operator that fails to provide notice to or register with Roskomnadzor is subject to administrative sanctions pursuant to the Code on Administrative Offenses of the Russian Federation.¹⁴⁸

Ensuring the security of PII is the responsibility of the data operator (generally, the employer).¹⁴⁹ Consequently, prior to transferring the PII to the employer’s server outside the territory of the Russian Federation, the employer must assure itself that the foreign country in which the server is located ensures the adequate protection of the PII.¹⁵⁰ Whether a foreign country adequately protects PII is generally determined on the basis of whether that country is a signatory to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, dated January 28, 1981 (the “Convention”).¹⁵¹ The Russian Federation is a signatory to the Convention; the United States is not.¹⁵²

Breaches of the Russian data protection laws (through illegal collection and dissemination of PII without the consent of the data subject) may result in criminal liability under various provisions of the Criminal Code of the Russian Federation.¹⁵³ Penalties may include monetary fines; prohibition on holding certain positions or performing certain activities; compulsory community work or correctional work; arrest; and/or imprisonment.¹⁵⁴ Criminal liability may be imposed on

individuals only (for example, the director or manager of the data operator).¹⁵⁵

Q 12.15 Do other foreign laws affect the collection and use of information besides those relating to the protection of PII?

In addition to legislation regarding PII, foreign blocking statutes—which regulate, and in some instances criminalize, the collection and exportation of information requested in the course of foreign legal proceedings—may place conflicting obligations on litigants or other participants in U.S. judicial or regulatory proceedings. While data privacy legislation is intended to protect the personal information of individuals, foreign blocking statutes are intended to protect the sovereignty of the state and its citizens from foreign litigation.

For example, the French blocking statute, French Penal Code Law No. 80-538, prohibits requests for, or disclosure of, documents or information sought as part of discovery in foreign litigation, except in connection with proceedings under the Hague Convention.¹⁵⁶ Failure to comply with this law may result in the imposition of penalties ranging from monetary fines to imprisonment.¹⁵⁷ Similarly, under the U.K. blocking statute, the Protection of Trading Interests Act, the U.K. Secretary of State is authorized to prohibit discovery where it conflicts with the trading interests or infringes on the sovereignty of the U.K.¹⁵⁸ Other countries with similar blocking statutes include Sweden, the Netherlands, Japan, Australia and Canada.¹⁵⁹

Most recently, China passed a “Personal Information Protection Law” (PIPL) that entered into effect on November 1, 2022. PIPL contains new rules that appear designed to restrict transfers of personal data from China to the U.S. (or any other non-Chinese jurisdiction) for purposes of litigation or regulatory enforcement. Under Article 41 PIPL, companies “may not provide personal information stored within the mainland territory of the People’s Republic of China to foreign judicial or law enforcement agencies.”¹⁶⁰ Instead, the “[c]ompetent authorities of the People’s Republic of China” are to “handle foreign judicial or law enforcement authorities’ requests regarding the provision of personal information stored domestically [i.e. within mainland China].”¹⁶¹ This provision suggests that Chinese entities—or

non-Chinese entities who store data in mainland China—may not be able to produce personal data to the SEC in response to an SEC request, and would instead need to route such a request to competent Chinese legal or diplomatic authorities for resolution. Article 41’s rules may also be invoked more broadly by companies that are located within China, or whose data is located within China, as grounds for refusing to produce documents in connection with SEC investigations or related litigation. Though the case law interpreting PIPL is nascent, U.S. courts have to date uniformly rejected arguments that PIPL excuses failures to produce discoverable documents.¹⁶²

Q 12.16 How does one typically comply with conflicting obligations to produce documents to the SEC and the data protection laws in foreign jurisdictions?

Foreign or global litigants may invoke the blocking statute(s) of their home jurisdiction, or the jurisdiction where the requested information is located, in an attempt to avoid producing documents or witnesses in U.S. proceedings and/or limit the scope of the production or testimony. As a consequence, additional proceedings in the United States and the jurisdiction that has enacted the blocking statute may be commenced to determine the parties’ respective discovery-related rights and obligations. At that point, litigants may decide it is in their best interest to wait for a ruling by one or more of these jurisdictions before determining whether and how to respond to discovery requests in U.S. proceedings.

Q 12.17 Does the United States defer to foreign blocking statutes?

U.S. courts—which are not bound to follow foreign law—employ a comity analysis in determining whether the interests of litigants or participants that seek to obtain discovery in U.S. proceedings outweigh the interests of foreign state sovereignty. In conducting this comity analysis, U.S. courts consider seven factors: (1) the importance of the discovery sought, relative to the litigation; (2) the degree of specificity of the discovery request; (3) whether the requested information originated in the United States or abroad; (4) whether alternate means of obtaining the requested information exist; (5) the

extent to which noncompliance with the request would undermine the interests of the United States and the interest of any state where the information sought is located or found; (6) whether the party resisting discovery has acted in good faith; and (7) any hardship that would result from compliance with discovery.¹⁶³

Not surprisingly, a number of U.S. courts have found that the application of these factors weighed in favor of production of the requested information. For example, in *In re Global Power Equipment Group, Inc.*, the court held that principles of comity weighed in favor of compliance with the Federal Rules of Civil Procedure, notwithstanding the possibility of criminal penalties under the French blocking statute.¹⁶⁴ The *Global Power* court acknowledged that the case—a U.S. bankruptcy proceeding in which the production of documents and witnesses located in the Netherlands, France and Belgium was sought by the plan administrator in connection with proofs of claim filed by a French company against the bankrupt entity—did not implicate broader U.S. interests.¹⁶⁵ Nonetheless, the court found that because the information sought was “central to resolving the contested matter[,]” and because the United States had an interest in “securing the prompt, economical and orderly administration of its bankruptcy cases[,]” the facts of the *Global Power* case weighed in favor of the application of the Federal Rules.¹⁶⁶

Global Coordination

Q 12.18 How have international investigations changed in the wake of the financial crisis?

The global economic downturn spurred regulators around the world, including the SEC, to a new level of aggressiveness. These regulators have sought increased cooperation and communication with their foreign counterparts, in order to work effectively in a financial world dominated by multinationals and interconnected by global markets. The global reach of the SEC and other regulators presents new challenges for U.S. entities that operate abroad and for non-U.S. entities that operate or publicly trade in the United States.¹⁶⁷

The cooperation between regulators in the U.S. and the U.K. serves as an archetype of the across-the-board rise in cooperation

amongst regulators across the globe. Both the U.S. and the U.K. place the enforcement of securities laws within the purview of a central authority, which promotes efficient cross-border cooperation.¹⁶⁸ Of course, in the United States, the SEC holds that central role. In 2013, the U.K. government transferred the enforcement powers of its chief financial regulator, the Financial Services Authority (FSA), to a new entity, the FCA.¹⁶⁹

In contrast to the direct lines of communication that exist between regulators in the U.S. and the U.K., communication and cooperation between regulators in the U.S. and the EU necessarily involves additional complications, as no central authority exists in the EU to oversee enforcement of securities laws across the EU Member States. As a result, U.S. regulators must manage relationships and reach agreements with the various EU Member States on an individual basis, which presents administrative hurdles.

The trend toward greater international cooperation between regulators in the U.S. and the U.K. extends beyond the enforcement of securities laws and includes the enforcement of laws related to money laundering, antitrust, bribery and export control, among others. Practitioners should counsel U.S. clients that operate in the U.K., and U.K. entities that operate in the U.S., to expect a further upswing in cross-border regulation and enforcement.

The most recent example of this trend is the U.S.-U.K. agreement on “Access to Electronic Data for the Purpose of Countering Serious Crime,” which the two governments signed in October 2019.¹⁷⁰ Under this agreement, law enforcement authorities can skip the traditional (and often drawn-out) MLAT process by petitioning a domestic court to issue an overseas production order (OPO) that compels the production of electronic data stored across the Atlantic Ocean. This means that U.K. law enforcement—the primary beneficiary under the law since most of the data at issue is located within the United States—can obtain an OPO from a U.K. court that requires a U.S. communications service provider to produce electronic data.

**CASE STUDY: *Libor Investigation***

The investigation into alleged manipulation of the London Interbank Offered Rate (“Libor”) at Barclays plc provides an illustrative example of the effective cooperation between authorities in the U.S. and the U.K.¹⁷¹ In the U.K., the FSA led the inquiry. In the U.S., separate investigations were launched by the Commodity Futures Trading Commission (CFTC), the DOJ and the SEC. To facilitate the cross-border cooperation required, the DOJ received relevant documents from the FSA under an MLAT.¹⁷²

The investigation into Libor started in earnest in 2008, after a number of articles appeared in *The Wall Street Journal* that questioned whether banks on the Libor submission panel, including Barclays, submitted Libor rates below the banks’ actual cost of funds in the London interbank market, in order to reduce the banks’ reputational risk.¹⁷³ As the investigation developed, another form of alleged manipulation came to light—efforts by traders to affect the official Libor set, through coordination with traders at other panel banks, in order to benefit the traders’ own books.¹⁷⁴

In June 2012, Barclays became the first major bank to settle with authorities in the U.S. and the U.K. over claims of alleged Libor manipulation, when it reached separate and contemporaneous settlements with each of the U.S. and U.K. authorities involved.¹⁷⁵ Pursuant to the settlements, Barclays agreed to pay, respectively, a \$200 million fine to the CFTC (at the time, the largest penalty ever levied by that body), a \$160 million fine to the DOJ and a \$59.5 million fine to the FSA.¹⁷⁶ Although Barclays avoided any criminal charges, the settlement required the bank to admit that traders and officers of the bank engaged in manipulation.¹⁷⁷ Barclays also agreed to continue its cooperation with the authorities, which the settlement documents highlighted as a factor considered when assessing the financial penalties.¹⁷⁸

Notably, the global Libor benchmark rate manipulation investigation also gave rise to an important development under U.S. law when, in July 2017, the U.S. Court of Appeals for the Second Circuit vacated the criminal convictions and dismissed the indictment of two former Libor submitters from Rabobank on Fifth Amendment grounds.¹⁷⁹ Although neither defendant was a U.S. citizen, the Second Circuit concluded that, because they had been compelled to testify in a foreign regulatory proceeding by the U.K. FCA, and because their interviews had then been reviewed by a cooperating defendant in their U.S. prosecution, the taint associated with such Fifth Amendment violations undercut not only their convictions, but also their indictment.¹⁸⁰ In particular, the Second Circuit ruled that the Fifth Amendment's prohibition against the use of compelled testimony applies even if the testimony was compelled by a foreign sovereign that was, at the time, under no obligation to avoid self-incrimination.¹⁸¹ Applying *Kastigar v. United States*,¹⁸² the Second Circuit further held that the Justice Department had failed to meet the "heavy burden" of showing that a cooperating defendant's testimony had not been shaped, altered, or affected by his review of the defendants' FCA interview transcripts.¹⁸³

Q 12.19 What particular challenges do practitioners face in light of the increased international cooperation amongst regulators?

The need to coordinate investigations with regulators in several countries and, potentially, to negotiate a settlement with each of those regulators, presents the greatest challenge to attorneys and their clients. In light of the public and media attention paid to cross-border investigations, regulators may compete with one another to secure the highest penalty from the subject of the investigation and, therefore, seek to gain leverage by holding out for a separate settlement. Similarly, a regulator may face unique political pressures in its home country, which affects its willingness or even its ability to enter into a global settlement.

Ideally, an entity or individual subject to a cross-border investigation would reach contemporaneous settlements with the entire group of regulators involved, rather than a piecemeal settlement over an extended period. JPMorgan recently fell short of this preferred outcome, however, when it settled claims that it failed to adequately supervise traders who incurred, and then tried to hide, large trading losses. From 2007 through 2012, the Chief Investment Officer (CIO) at JPMorgan accumulated a large position in credit default indices.¹⁸⁴ The credit default indices were tied to various credit default swaps—a financial instrument that acts as an insurance policy or hedge against a borrower’s potential default on a loan or other obligation.¹⁸⁵ At the end of 2011, the portfolio managed by the CIO contained over \$50 billion notional in credit default indices, which the firm had accumulated, in large part, through the efforts of one CIO trader in London, whom the press eventually referred to as the “London Whale.”¹⁸⁶

At the end of February 2012, traders in the CIO realized that the position in credit default indices, which included a very large short position, would likely suffer catastrophic losses if market trends continued.¹⁸⁷ To avert the predicated losses, traders in the CIO decided to “defend” the short position in credit default indices.¹⁸⁸ This strategy required the traders to sell a substantial number of securities to put downward pressure on the market price, which would benefit the short position of the CIO portfolio.¹⁸⁹ Specifically, on February 29, 2012, the CIO sold, on net, more than \$7 billion of a particular credit default index, which, as the traders planned, substantially forced down the market price.¹⁹⁰ Despite this effort, however, the position continued to lose value, and, in an attempt to hide the size of the mounting losses, the traders changed the method used to mark the portfolio to market, which overstated the position’s value.¹⁹¹ Ultimately, JPMorgan reported losses of approximately \$6 billion and had to restate its previously released financial statements for the first quarter of 2012.¹⁹²

In September 2013, JPMorgan agreed to pay a total of over \$920 million in penalties to four regulators: \$200 million to the SEC; \$300 million to the U.S. Office of the Controller of the Currency; \$200 million to the U.S. Federal Reserve; and \$222 million to the FCA.¹⁹³ The settlement with the SEC also required JPMorgan to admit that it

had violated federal securities laws by, among other things, its failure to adequately supervise the traders involved.¹⁹⁴

As noted, unlike Barclays, JPMorgan failed to reach a contemporaneous settlement with each of the several regulators that investigated its conduct. Specifically, the September 2013 settlement did not involve the CFTC, and the CFTC sought an admission of wrongdoing related to the actual trades involved, separate from the inadequate supervision that JPMorgan previously admitted.¹⁹⁵ To support its position, the CFTC relied on a key provision of the Dodd-Frank Act.¹⁹⁶ That provision prohibits the use of “any manipulative or deceptive device” in connection with a swap or futures contract.¹⁹⁷ The scienter or state-of-mind required for the offense includes recklessness.¹⁹⁸ When JPMorgan and the CFTC eventually reached a settlement, in October 2013, JPMorgan admitted that its traders acted recklessly when they tried to protect the doomed short position.¹⁹⁹ Under the terms of the settlement, JPMorgan paid an additional \$100 million in monetary penalties and agreed to implement enhancements to its supervision and control systems.²⁰⁰ In the press release that accompanied the settlement, the CFTC acknowledged the assistance provided by the FCA, as well as the SEC and the U.S. Attorney’s Office for the Southern District of New York.²⁰¹

Q 12.20 What problems could develop as the SEC and other regulators seek to extend their enforcement of U.S. securities laws outside the borders of the United States?

Predictably, some countries resent the effort by the SEC to extend the reach of U.S. securities laws and policies abroad. Therefore, not all cross-border matters result in friendly cooperation between U.S. and foreign regulators or in eventual settlement. For example, in May 2012, the SEC charged Shanghai-based Deloitte Touche Tohmatsu CPA Ltd. for its refusal to provide audit work papers related to a Chinese company under investigation by the SEC. The SEC alleged that the Chinese Deloitte affiliate violated a provision in the 2002 Sarbanes-Oxley Act that requires foreign public accounting firms to provide, upon SEC request, work papers that concern companies that publicly trade in U.S. markets. In 2010, the firm had provided the work papers to the Chinese Securities Regulatory Commission, which had acted

in response to a SEC request. The SEC and the Chinese Securities Regulatory Commission, however, had been unable to reach an agreement that would result in the delivery of the work papers to the SEC. Therefore, the Chinese Deloitte affiliate found itself in an unenviable position, caught in the middle of a disagreement between two sovereign nations. In late January 2014, an ALJ with the SEC ruled that Deloitte Touche Tohmatsu CPA Ltd., among others, had violated U.S. rules by failing to turn over its work papers related to audits of Chinese companies under SEC investigation. The trial judge recommended the Chinese affiliates be suspended from auditing Chinese companies listed in the United States for six months. Shortly thereafter, the SEC and Deloitte Touche Tohmatsu CPA Ltd. filed a joint motion to dismiss, without prejudice, the subpoena enforcement action that the SEC filed against Deloitte Touche Tohmatsu CPA Ltd. The SEC agreed to dismiss the enforcement action after the Chinese Securities Regulatory Commission turned over a substantial number of documents to the SEC. The resolution of this discovery dispute did not resolve the larger administrative action.

Notably, in 2020, Congress passed the Holding Foreign Companies Accountable Act (HFCAA).²⁰² The HFCAA was passed, in part, in response to decade-long interference from local authorities in China and Hong Kong with U.S. investigations and audits. “[O]nce an issuer is identified as a Commission-Identified Issuer for two consecutive years, the Commission is required under the HFCAA to prohibit the trading of the issuer’s securities on a national securities exchange and in the over-the-counter market.”²⁰³

U.S. regulators continue to assert jurisdiction over foreign corporations that trade in the U.S. Attorneys that represent such clients should take note of that fact and advise the client on the need to comply with U.S. securities laws. Attorneys should also anticipate the difficulty in complying with U.S. law if the relevant law conflicts with the laws of the company’s home jurisdiction. For that reason, the U.S. attorney should, upon the engagement of the foreign client, familiarize him or herself with the laws of the foreign jurisdiction and consult with foreign counsel as soon as possible.

The SEC also recently obtained a significant ruling regarding its ability to regulate the foreign transactions of domestic companies. In *SEC v. Scoville*,²⁰⁴ the U.S. Court of Appeals for the Tenth Circuit

concluded that the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) essentially codified the old “conduct-and-effects” test—previously repudiated by the Supreme Court in its 2010 *Morrison* decision²⁰⁵—for determining whether the antifraud provisions of the federal securities acts reach extraterritorial sales. The Tenth Circuit first analyzed the relevant provision of Dodd-Frank, and concluded that it affirmatively “indicated that the antifraud provisions should apply extraterritorially when the statutory conduct-and-effects test is met.”²⁰⁶ The court then held that the defendant’s sales to foreign investors satisfied the test because the defendant promoted the investments over the internet while residing in Utah and his servers were physically located in the United States.²⁰⁷

Given the potential breadth of the conduct-and-effects test (as seen through pre-*Morrison* case law),²⁰⁸ the *Scoville* reasoning has the potential to greatly increase the SEC’s ability to bring extraterritorial enforcement actions under the federal securities acts. To the extent other courts agree with the Tenth Circuit’s interpretation of Dodd-Frank, *Morrison* will no longer provide foreign entities and investors with the same level of protection against the SEC.

Q 12.21 What areas outside of securities regulation have experienced a rise in international cooperation between regulators?

The effort to combat corruption has benefited from the continued growth in regulatory cooperation and enforcement. In 2016, the SEC initiated more than thirty enforcement actions related to alleged Foreign Corrupt Practices Act (FCPA) violations, and, for its part, the DOJ initiated approximately twenty separate prosecutions.²⁰⁹ In 2016, corporate fines in FCPA cases topped \$2 billion for the first time in the history of the FCPA.²¹⁰ In 2013, one of the largest settlements ever at the time, in the amount of \$398 million, involved the first coordinated action by U.S. and French authorities in a major foreign bribery case.²¹¹ In 2014, one settlement with the DOJ in the amount of \$772 million involved coordination between authorities in the United States, Indonesia, Switzerland, the U.K., Germany, Italy, Singapore, Saudi Arabia, Cyprus, and Taiwan.²¹² The SEC’s continued commitment to FCPA enforcement was seen in 2022 through charges against Credit Suisse Group, charges against Oracle Corporation, and

charges against Tenaris for FCPA violations.²¹³ Additionally, in 2022, the SEC filed 760 total enforcement actions—a 9% increase from 2021.²¹⁴ And, “[t]he fight against foreign corruption is a top priority for the Biden Administration . . . and a core national security interest.”²¹⁵ In recent years, the DOJ has cooperated with many foreign partners, including the U.K., Brazil, Malaysia, Switzerland, Ecuador, France, the Netherlands, and Singapore, in this fight against foreign corruption.²¹⁶ For example, Malaysian authorities worked closely with the DOJ in the Goldman Sachs 1MDB scandal, in which “billions of dollars were stolen from a Malaysian sovereign wealth fund meant to promote the country’s economic development.”²¹⁷ As part of the resolution, over \$1.2 billion was repatriated to the Malaysian people.²¹⁸

In December 2016, the SEC and DOJ announced separate settlements with international conglomerate Teva Pharmaceutical Industries Limited related to allegations that Teva paid bribes to foreign government officials in Russia, Ukraine, and Mexico.²¹⁹ As part of its settlement, Teva agreed to pay more than \$236 million in disgorgement and interest to the SEC plus a \$283 million penalty in a deferred prosecution agreement with the DOJ.²²⁰ Additionally, Teva was required to retain an independent corporate monitor for at least three years.²²¹ Also in 2016, the SEC and DOJ entered into a global settlement with Odebrecht S.A., a Brazilian construction conglomerate and Braskem S.A., a Brazilian petrochemical company, totaling \$3.5 billion in total penalties among authorities in the United States, Brazil, and Switzerland arising out of their scheme to pay millions of dollars in bribes to government officials around the world.²²² This resolution now stands as the largest global foreign bribery settlement of all time.²²³ As part of the settlement, Odebrecht agreed to pay approximately \$260 million to the DOJ, while Braskem agreed to pay approximately \$95 million to the DOJ and \$65 million to the SEC.²²⁴ The remainder is to be paid to authorities in Brazil and Switzerland.²²⁵

Several important recent developments in the law and policy governing FCPA enforcement bear mentioning. With regard to governing law, in July 2018, the district court in *SEC v. Cohen* applied the five-year statute of limitations under 28 U.S.C. § 2462 to dismiss an SEC FCPA enforcement action.²²⁶ In doing so, the trial court invoked the U.S. Supreme Court’s reasoning in *SEC v. Kokesh*²²⁷ to find that SEC requests for prospective injunctive relief—so-called “obey the law

injunctions”—are at least partially punitive such that they, like the SEC’s parallel FCPA claims for disgorgement and civil penalties, accrue at the time a bribe is paid (rather than when contract benefits are realized) and are not subject to equitable tolling.²²⁸

In August 2018, the U.S. Court of Appeals for the Second Circuit held in *United States v. Hoskins* that theories of accessory or ancillary liability are legally unavailable to expand the scope of individuals statutorily subject to SEC or DOJ jurisdiction under the FCPA.²²⁹ In particular, the Second Circuit concluded that the categories of individuals and entities subject to FCPA jurisdiction had been narrowly drawn by Congress so as to indicate an affirmative legislative policy not to reach, specifically including on a conspiracy or accessory basis, individual foreign nationals who engage in corrupt activity outside the United States while employed by or acting as an agent of a foreign company.²³⁰ Applying the Second Circuit’s ruling on remand, the district court granted Hoskins’ motion for acquittal because the government had failed to prove that Hoskins acted as an agent of the relevant domestic entity.²³¹ It remains to be seen whether the *Hoskins* reasoning will be extended to afford corporations an FCPA defense based on agency principles.²³²

The DOJ has also made four important policy announcements with respect to FCPA enforcement over the past three years. First, in November 2017, the DOJ announced its FCPA enforcement policy, codifying a presumption against prosecution if a company self-discloses corrupt activity, fully cooperates in the government’s investigation, and remediates through, among other things, termination of culpable personnel and the adoption of compliance improvements.²³³ The FCPA enforcement policy also provides for a 50% reduction from the fine guideline range set by U.S. Sentencing Guidelines, assuming corporate self-disclosure, cooperation, and remediation.²³⁴ Second, in July 2018, DOJ announced extension of its FCPA enforcement policy to merger and acquisition transactions, facilitating disclosure by acquiring/successor companies of corrupt activity discovered through due diligence or post-acquisition.²³⁵ Third, in October 2018, DOJ issued a formal memorandum clarifying that imposition of a corporate monitor to resolve corporate criminal liability (including under the FCPA) is disfavored “[w]here a corporation’s compliance program and controls are demonstrated to be effective and appropriately resourced at the

time of resolution.”²³⁶ And finally, in November 2018, DOJ relaxed the requirement that companies disclose the identity of all individuals involved in criminal activity as a condition precedent to the extension of cooperation credit.²³⁷ DOJ policy now provides that cooperating companies need only disclose the identity of those “substantially involved” in criminal activity to obtain cooperation credit.²³⁸ Taken together, these policy pronouncements demonstrate the DOJ’s desire to foster self-disclosure, cooperation, and remediation without the corresponding fear that the government will deny cooperation credit and seek to impose a monitorship as a result.

More recently, the DOJ and SEC released an updated FCPA Resource Guide on July 3, 2020.²³⁹ This is the first update to the guide since its original publication in 2012. The update provides valuable insight into how the enforcement agencies view recent updates in the law. For example, the guide downplays the *Hoskins* decision (analyzed above), limiting its application to the Second Circuit and stating that “one district court from another circuit has rejected the reasoning in the *Hoskins* decision[.]”²⁴⁰

Q 12.22 What areas beyond corruption prevention have experienced a rise in international cooperation among regulators?

In addition to the enforcement of anti-corruption laws, U.S. authorities have continued to work with foreign governments to enforce U.S. tax laws and to identify undeclared assets of U.S. citizens in overseas accounts. In 2013, one of the most politically charged cross-border tax investigations moved towards a possible conclusion when the DOJ and the Swiss Federal Department of Finance announced a settlement program that offered amnesty from criminal prosecution to Swiss banks that self-reported possible tax-related offenses under U.S. law.²⁴¹ This announcement followed a program unveiled by the Swiss government, in the spring of 2013, that allowed Swiss banks under investigation by the DOJ to turn over data on Swiss bank accounts held by U.S. citizens—a break from the country’s traditional bank privacy laws.²⁴² These developments have allowed the DOJ to begin assessing, on an individual basis, the culpability of banks that elect to participate in the program, with an eye towards possible settlement of civil claims against culpable banks. For example, the DOJ announced in early 2016

that it had imposed more than \$1.3 billion in penalties on eighty banks since March 2015 under the program.²⁴³

In 2018, the Joint Chiefs of Global Tax Enforcement, or the “J5,” was formed.²⁴⁴ The J5 includes: the Australian Taxation Office (ATO), the Canada Revenue Agency (CRA), the Netherlands’ Fiscale Inlichtingen—en Opsporingsdienst (FIOD), the U.K.’s HM Revenue & Customs (HMRC), and the U.S.’s IRS Criminal Investigation.²⁴⁵ The purpose of the J5 is to combat transnational tax crime by increasing enforcement collaboration, increasing data and information sharing, increasing the capacity of enforcement officials, and sharing intelligence.²⁴⁶

Notes to Chapter 12

1. 15 U.S.C. § 78u(a).
2. *Id.* § 78u(b) (“[A]ny member of the Commission or any officer designated by it is empowered to administer oaths and affirmations, subpoena witnesses, compel their attendance, take evidence, and require the production of any books, papers, correspondence, memoranda, or other records which the Commission deems relevant or material to the inquiry.”).
3. *See* CFTC v. Nahas, 738 F.2d 487, 491 (D.C. Cir. 1984) (refusing to enforce an investigative subpoena served on a foreign citizen in a foreign state).
4. *See* 31 U.S.C. § 5318(k)(3)(A)(i); *In re* Grand Jury Proceedings (Bank of Nova Scotia), 691 F.2d 1384 (11th Cir. 1982).
5. SEC, DIV. OF ENF’T, ENFORCEMENT MANUAL § 3.3.6.2 (2017) [hereinafter ENFORCEMENT MANUAL], www.sec.gov/divisions/enforce/enforcementmanual.pdf.
6. INT’L ORG. OF SEC. COMM’NS, MULTILATERAL MEMORANDUM OF UNDERSTANDING CONCERNING CONSULTATION AND COOPERATION AND THE EXCHANGE OF INFORMATION (May 2012), www.iosco.org/library/pubdocs/pdf/IOSCOPD386.pdf.
7. *Id.* ¶ 7(b).
8. *Id.* ¶ 10(a)(ii).
9. *See id.* App. A.
10. Press Release, SEC, SEC and CFTC Participate in the Signing Ceremony for the IOSCO Enhanced Multilateral Memorandum of Understanding Concerning Cross-Border Enforcement (May 20, 2019), <https://www.sec.gov/news/press-release/2019-71>.
11. Int’l Org. of Sec. Comm’ns (IOSCO), Enhanced Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (EMMoU), <https://www.iosco.org/about/?subsection=emmou>.
12. Int’l Org. of Sec. Comm’ns (IOSCO), Signatories to EMMoU (last accessed January 11, 2023), <https://www.iosco.org/about/?subSection=emmou&subSection1=signatories>.
13. *See, e.g.*, Mutual Assistance in Criminal Matters art. 4, U.S.-Switz., May 25, 1973, 27 U.S.T. 2019; Judicial Assistance: Criminal Investigations art. 6(1), U.S.-Neth., June 12, 1981, 35 U.S.T. 1361.
14. For example, the MLAT between the United States and the European Union requires the parties to provide assistance to “a national administrative authority, investigating conduct with a view to criminal prosecution of the conduct, or referral of the conduct to criminal investigation or prosecution authorities. . . .” Agreement on Mutual Legal Assistance between the United States of America and the European Union art. 8 § 1, U.S.-EU, June 25, 2003, T.I.A.S. No. 10-201.1.

SEC COMPLIANCE AND ENFORCEMENT AB 2023

15. See Convention of 18 Mar. 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters, opened for signature Mar. 18, 1970, 28 U.S.T. 2555, T.I.A.S. No. 7444.

16. See *id.* art. 1.

17. See *id.* (requiring a “judicial authority” of a signatory state to issue a Letter of Request to obtain evidence abroad).

18. See *Intel Corp. v. Advanced Micro Devices, Inc.*, 542 U.S. 241, 247 n.1 (2004) (“[A] letter rogatory is the request by a domestic court to a foreign court to take evidence from a certain witness.”) (emphasis and citations omitted).

19. See 28 U.S.C. § 1781(b) (authorizing U.S. courts to transmit and receive letters rogatory or letters of request); FED. R. CIV. P. 28(b) (authorizing the taking of depositions abroad pursuant to letters rogatory); *Barnes & Noble, Inc. v. LSI Corp.*, No. C 11-02709 EMC LB, 2012 WL 1808849, at *2 (N.D. Cal. May 17, 2012) (“[a] court has inherent powers to issue letters rogatory”); *United States v. Staples*, 256 F.2d 292, 292 (9th Cir. 1958) (same). Section 1781 also empowers the Department of State to transmit and receive letters rogatory or letters of request, either “directly” or “through suitable channels.” 28 U.S.C. § 1781(a).

20. See 22 C.F.R. § 92.66(b) (“Letters rogatory may often be sent direct from court to court.”).

21. *Id.*

22. See U.S. DEP’T OF STATE, BUREAU OF CONSULAR AFF., Preparation of Letters Rogatory, <https://travel.state.gov/content/travel/en/legal/travel-legal-considerations/internl-judicial-asst/obtaining-evidence/Preparation-Letters-Rogatory.html>.

23. See *id.*; 22 C.F.R. § 92.54.

24. See U.S. DEP’T OF STATE, *supra* note 22.

25. See *id.* However, FED. R. CIV. P. 28(b)(4) provides that evidence obtained in response to a letter of request or letter rogatory “need not be excluded merely because it is not a verbatim transcript, because the testimony was not taken under oath, or because of any similar departure from the requirements for depositions taken within the United States.”

26. See ENFORCEMENT MANUAL, *supra* note 5, § 3.3.6.2.

27. Ian L. Schaffer, *An International Train Wreck Caused in Part by a Defective Whistle: When the Extraterritorial Application of SOX Conflicts with Foreign Laws*, 75 FORDHAM L. REV. 1829, 1835 & n.53 (2006).

28. *Id.*

29. See U.S. DEP’T OF STATE, *supra* note 22.

30. *United States v. Schwimmer*, 892 F.2d 237, 243 (2d Cir. 1989).

31. See Case C-550/07, *Akzo Nobel Chems. Ltd. and Akcros Chems. Ltd. v. Comm’n of the European Cmtys.*, 2010 E.C.R. 00000 (holding that attorney-client privilege is inapplicable where in-house counsel “does not enjoy the same degree of independence from his employer as a lawyer working in an external law firm does in relation to his client”); see also Case 155/79, *AM & S Eur., Ltd. v. Comm’n of the European Cmtys.*, 1982 E.C.R. 1575 (holding that privilege is not available where lawyer was “bound to the client by a relationship of employment”). *But see*

ECLI:NL:HR:2022:760 (clarifying the conditions under which in-house counsel in the Netherlands may invoke attorney-client privilege).

32. *Gucci Am., Inc. v. Guess?, Inc.*, 271 F.R.D. 58, 65 (S.D.N.Y. 2010).

33. *Anwar v. Fairfield Greenwich Ltd.*, 982 F. Supp. 2d 260, 264 (S.D.N.Y. 2013) (quoting *Astra Aktiebolag v. Andrx Pharm., Inc.*, 208 F.R.D. 92, 98 (S.D.N.Y. 2002)) (internal quotation marks omitted).

34. *Id.*

35. *AstraZeneca LP v. Breath Ltd.*, No. 08-1512, 2011 WL 1421800, at *1 (D.N.J. Mar. 31, 2011).

36. *Id.* at *5.

37. *Id.* at *8.

38. *Veleron Holding, B.V. v. BNP Paribas SA*, No. 12-cv-5966, 2014 WL 4184806, at *5 (S.D.N.Y. Aug. 22, 2014).

39. *Id.*

40. *Id.* at *6.

41. *Id.*

42. *Id.*

43. *See Renfield Corp. v. E. Remy Martin & Co., S.A.*, 98 F.R.D. 442 (D. Del. 1982).

44. *See id.* at 444.

45. *See id.* at 444–45.

46. *See id.* at 445. *See also* *Sudenga Indus. v. Global Indus.*, 2020 U.S. Dist. LEXIS 85692, at *7–10 (D. Kan. May 15, 2020) (reaching same conclusion).

47. Client Memorandum by Willkie Farr & Gallagher LLP, *Beware: Legal Privilege Rules Differ Between the U.S. and the EU* (June 19, 2008), www.willkie.com/~media/Files/Publications/2008/06/Beware%20%20Legal%20Privilege%20Rules%20Differ%20Between%20the_/Files/LegalPrivilegeRulesDifferBetweenUSandEU.pdf/FileAttachment/LegalPrivilegeRulesDifferBetweenUSandEU.pdf.

48. *See* Case 155/79, *AM & S Eur., Ltd. v. Comm’n of the European Cmtys.*, 1982 E.C.R. 1575.

49. *See id.* ¶ 21.

50. *See id.* ¶ 25.

51. *See* Case C-550/07, *Akzo Nobel Chems. Ltd. & Akcros Chems. Ltd. v. Comm’n of the European Cmtys.*, 2010 E.C.R. 00000.

52. *See id.* ¶¶ 14, 47–51.

53. *See* Council Regulation (EC) No. 1/2003, art. 20, O.J. (L 1) 04/01/2003.

54. *See In re Parmalat Sec. Litig.*, No. 04 MD 1653, 2006 WL 3592936, at *4 (S.D.N.Y. Dec. 1, 2006); *see also* FED. R. EVID. 502.

55. *See, e.g., In re Sealed Case*, 877 F.2d 976, 980 (D.C. Cir. 1989) (“Short of court-compelled disclosure or other equally extraordinary circumstances, we will not distinguish between various degrees of ‘voluntariness’ in waivers of the attorney-client privilege.”) (citation and footnote omitted).

56. *See, e.g., In re Vitamin Antitrust Litig.*, Misc. No. 99-197, 2002 WL 35021999, at *28 (D.D.C. Jan. 23, 2002) (finding defendants disclosed documents to European

SEC COMPLIANCE AND ENFORCEMENT AB 2023

Commission voluntarily after defendants failed to show that defendants objected to disclosure and that failure to respond would have subjected defendants to sanctions).

57. *Parmalat*, 2006 WL 3592936, at *3.

58. *Id.*

59. *See id.* at *4.

60. *See id.*

61. *See id.* at *5–7.

62. *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 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”), Official Journal of the European Union L 119 at 1–88 (May 4, 2016). The European Economic Area includes all member states of the EU, as well as Iceland, Liechtenstein, and Norway.

63. *See* [Act on the Protection of Personal Information], Act No. 57 of 2003, *translation at* www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf (enacted in 2003 and effective as of Apr. 1, 2005).

64. *See* Personal Information Protection Law of the People’s Republic of China, passed Aug. 20, 2021, *translation at* <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>.

65. *See* Lei No. 13.709 de 14 de Agosto de 2018 (Lei Geral de Proteção de Dados Pessoais [General Personal Data Protection Law]), http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm.

66. *See* Federal Law on Personal Data, July 27, 2006, No. 152-FZ [hereinafter PD Law], *translation at* https://iapp.org/media/pdf/knowledge_center/Russian_Federal_Law_on_Personal_Data.pdf.

67. *See* Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gen. S.R. & O. 313(E).

68. *See* Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

69. *See* Bundesgesetz über den Datenschutz [Federal Act on Data Protection], *translation at* https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/en.

70. *See* Article 31 of the UAE Constitution of 1971; UAE Federal Law No. 3 of 1987; Articles 378 and 379 of the UAE Penal Code.

71. *See* Ley Federal de Protección de Datos Personales en Posesión de Particulares [LFPDP] [Federal Law on the Protection of Personal Data Held by Private Parties], Diario Oficial de la Federación [DO], 5 de julio de 2010 (Mex.), *translation at* https://iapp.org/media/pdf/knowledge_center/Mexico_Federal_Data_Protection_Act_July2010.pdf.

72. *See* Computer Processed Personal Data Protection Law (Taiwan) (amended and retitled in 2010 as the Personal Information Protection Act).

73. See *Final Rule: Privacy of Consumer Financial Information (Regulation S-P)*, Exchange Act Release No. 42974, Investment Company Act Release No. 24543, Investment Advisers Act Release No. 188, www.sec.gov/rules/final/34-42974.htm.

74. *Id.*

75. *Id.*

76. See NEXTE Fin. Grp., Inc., Exchange Act Release No. 56316, 2007 WL 2409851 (Aug. 24, 2007); see also NEXTE Fin. Grp., Inc., Exchange Act Release No. 349, 2008 WL 2444775 (ALJ June 18, 2008).

77. See NEXTE Fin. Grp., Inc., Exchange Act Release No. 56316, 2007 WL 2409851 (Aug. 24, 2007).

78. Woodbury Fin. Servs., Inc., Exchange Act Release No. 59740, 2009 WL 960760 (Apr. 9, 2009) (Woodbury consented to the entry of the Order without admitting or denying any of the findings.).

79. Press Release, SEC, No. 2016-112, *Morgan Stanley Failed to Safeguard Customer Data* (June 8, 2016), www.sec.gov/news/pressrelease/2016-112.html.

80. *Id.*

81. See Press Release, SEC, No. 2011-86, *SEC Charges Brokerage Executives with Failing to Protect Confidential Customer Information*, www.sec.gov/news/press/2011/2011-86.htm.

82. *Id.*

83. *In re Craig Scott Capital, LLC*, Exchange Act. Release No. 77595, 2016 WL 1444441, at *1 (Apr. 12, 2016).

84. *Id.* at *5–6.

85. See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 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”), Official Journal of the European Union L 119 at 1–88 (May 4, 2016) [hereinafter GDPR].

86. See *id.* art. 94(1) (“Directive 95/46/EC [i.e., the Data Protection Directive] is repealed with effect from 25 May 2018.”).

87. See *id.* art. 83. The GDPR contains a two-tiered fining regime. Article 83(4) GDPR identifies a lower tier of violations that can be fined at up to €10 million or 2% of worldwide annual turnover, whichever is greater. More serious violations can be fined at a second tier of up to €20 million or 4% of worldwide annual turnover, whichever is greater. See *id.* art. 83(5). The legal issues discussed in this article can be sanctioned under the higher, second-tier fines.

88. See *id.* art. 82 (“Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation . . . for the damage suffered.”).

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

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

91. *See id.*

92. *See id.* art. 5(1)(b) (“Personal data shall be [] collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes . . . (‘purpose limitation’).”).

93. *See id.* art. 6(4) (permitting personal data to be “further processed” (i.e., re-used) for “another purpose [that] is compatible with the purpose for which the personal data [were] initially collected” if certain statutory prerequisites are satisfied).

94. *See id.* art. 6(4) (permitting personal data to be “further processed” (i.e., re-used) based on individuals’ consent).

95. *See, e.g.*, BETRIEBSVERFASSUNGSGESETZ (Works Constitution Act), Ch. 2 (permitting creation of works councils) (Ger.).

96. *See* GDPR, *supra* note 85, art. 88 (permitting EU Member States to “provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context, in particular . . . including discharge of obligations laid down by law or by collective agreements”). The GDPR’s recitals expressly recognize that “Member State law or collective agreements, including ‘works agreements’, may provide for specific rules on the processing of employees’ personal data in the employment context.” *See* GDPR Recital 155.

97. *See* GDPR, *supra* note 85, art. 6(1)(a).

98. *See id.* art. 6(1)(b).

99. *See id.* art. 6(1)(c).

100. *See id.* art. 6(1)(d).

101. *See id.* art. 6(1)(e).

102. *See id.* art. 6(1)(f).

103. *Id.* art. 4(11).

104. *Id.* art. 7(3) (“The data subject shall have the right to withdraw his or her consent at any time.”).

105. *See id.* art. 21 (setting forth the right to object to data processing which companies base on their legitimate interests).

106. *See id.* art. 21(1) (“The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1) The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds . . . for the establishment, exercise or defence of legal claims.”).

107. *See id.* art. 44 (“Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country . . . shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter [V of the GDPR] are complied with.”).

108. *See id.* art. 45(1) (“A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.”).

109. The countries currently recognized as providing adequate protection for EU data are: (1) Andorra, (2) Argentina, (3) Canada, (4) Faroe Islands, (5) Guernsey, (6) Israel, (7) Isle of Man, (8) Japan, (9) Jersey, (10) New Zealand, (11) Switzerland, and (12) Uruguay. *See* EUROPEAN COMM’N, *Adequacy Decisions: How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection*, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en#dataprotectionincountriesoutsidetheeu.

110. *See, e.g.*, U.S. DEP’T OF COMMERCE, INT’L TRADE ADMIN., PRIVACY SHIELD, *Benefits of Participation*, <https://www.privacyshield.gov/article?id=Benefits-of-Participation>.

111. *See* GDPR, *supra* note 85, art. 46(2)(c) (permitting transfers on the basis of “standard data protection clauses adopted by the [European] Commission”).

112. *See* EUROPEAN COMM’N, Commission decision 2004/915/EC of 27 Dec. 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, Clause II.(i)(ii)–(iii). Generally, companies who receive EU data under the Standard Contractual Clauses cannot transfer it to further recipients unless (a) the new recipient itself executes the Standard Contractual Clauses, or (b) affected individuals are notified of the intended transfer and provided with an opportunity to object. *See id.* If a U.S. affiliate has received personal data in the capacity of a “data processor” from EU affiliates, the Standard Contractual Clauses applicable to processors require the U.S. affiliate to promptly notify its EU affiliates about “any legally binding request for disclosure of the personal data by a law enforcement agency,” but they do not expressly prohibit such disclosure. *See* EUROPEAN COMM’N, Commission Decision of 5 Feb. 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, Clause 5(d)(i). However, EU courts have not weighed in on the issue. EU affiliates will see such a disclosure as creating GDPR enforcement risk subject to the sanctions discussed above. Counsel should thus continue to be willing to work with EU affiliates to create a defensible review and production structure.

113. *See* GDPR, *supra* note 85, art. 49(1) (permitting transfers based on derogations and setting forth GDPR-recognized derogations).

114. *See id.* art. 7.

115. *Id.* art. 49(1)(a). As a practical matter, consent declarations may memorialize the disclosures by which the declarant has been advised of these risks.

116. *Id.* art. 49(1)(e).

117. *See id.* art. 49(1).

118. *See* Data Prot. Comm'r v. Facebook Ireland Ltd & Maximilian Schrems, Case C-311/18 (E.C.J. July 16, 2020).

119. *See id.* ¶¶ 168–202.

120. *See id.* ¶ 202.

121. *See id.* ¶¶ 104–105.

122. *See* GDPR, *supra* note 85, art. 49(1)(a) (permitting transfers on the basis of consent).

123. *Id.* art. 49(1)(e).

124. *See* Letter from James Dipple-Johnstone to Raquel Fox (Sept. 11, 2020), <https://ico.org.uk/media/for-organisations/documents/2619110/sec-letter-20200911.pdf>.

125. *See generally* June 25, 2021, Memorandum Concerning Swiss Firm Data Processing and Sharing of Information with the U.S. Securities & Exchange Commission.

126. *Id.* § 1.2.

127. *Id.* §§ 1.2, 2.5.2.

128. *See* Eur. Data Prot. Bd., *Statement on the Court of Justice of the European Union Judgment in Case 3-11/18—Data Protection Commissioner v Facebook Ireland and Schrems at 2* (July 17, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20200717_cjeujudgmentc-311_18_en.pdf.

129. *Id.* at 2.

130. Arguments for a strict interpretation may reference the GDPR's recitals. *See, for example,* GDPR Recital 115, stating the following:

Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring [companies] to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation.

131. *See* *United States v. Microsoft Corp.*, 138 S. Ct. 1186.

132. *See id.* (vacating opinion on review and remanding to district court with instructions to dismiss the case as moot in light of the CLOUD Act).

133. See Brief for the European Comm'n on behalf of the European Union, as Amicus Curiae in Support of Neither Party, *United States v. Microsoft Corp.* 138 S. Ct. 1186 (2018) (No. 17-2), at 14.

134. See Brief for Bundesverband der Deutschen Industrie e.V., Deutscher Industrie- und Handelskammertag e.V. [Federation of German Industries] et al. as Amici Curiae in Support of Respondent, *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (No. 17-2), at 14.

135. See AGREEMENT BETWEEN THE GOVERNMENT OF THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND AND THE GOVERNMENT OF THE UNITED STATES OF AMERICA ON ACCESS TO ELECTRONIC DATA FOR THE PURPOSE OF COUNTERING SERIOUS CRIME (Oct. 3, 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

136. See, e.g., EUR. COMM'N, *Criminal Justice: Joint Statement on the Launch of EU-U.S. Negotiations to Facilitate Access to Electronic Evidence* (Sept. 26, 2019) (announcing the beginning of EU-U.S. negotiations).

137. See Arts. 9-10 GDPR.

138. Art. 9(2)(f) GDPR.

139. Art. 5(1)(c) GDPR.

140. See Regulation (EU) 2016/679 of the European Parliament and of the Council, <https://www.legislation.gov.uk/eur/2016/679/contents> [hereinafter UK GDPR].

141. See Art. 49(1)(e) UK GDPR.

142. U.K. Information Commissioner, *International Transfers*, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers>.

143. See Letter from James Dipple-Johnstone to Raquel Fox (Sept. 11, 2020), <https://ico.org.uk/media/for-organisations/documents/2619110/sec-letter-20200911.pdf>.

144. See PD Law, *supra* note 66, art. 3.

145. *Id.* arts. 6, 15. While the PD Law generally governs the activities of all sectors and organizations, it does not regulate the processing of PII exclusively for personal or family needs, unless such processing also violates the rights of other individuals. *Id.* art. 1(2).

146. *Id.* art. 6. Note that while the PD Law does not contain any express provisions on territorial effect, some commentators have taken the approach that the PD Law applies to both the processing of personal data located in Russia and the processing of personal data of Russian citizens or residents regardless of whether the data operator is located inside or outside of Russia.

147. See *Protecting the Rights of Personal Data Subjects*, ROSKOMNADZOR (Aug. 20, 2009), http://eng.rkn.gov.ru/personal_data/protecting_the_rights_of_personal_data_subjects/.

SEC COMPLIANCE AND ENFORCEMENT AB 2023

148. See *Regulatory Acts of the Federal Executive Authorities*, ROSKOMNADZOR, http://eng.pd.rkn.gov.ru/legislation_of_the_russian_federation/judicial_practice/.
149. See DLA PIPER, DATA PROTECTION LAWS OF THE WORLD—FULL HANDBOOK 636, www.dlapiperdataprotection.com.
150. *Id.*
151. *Id.* at 633, 636.
152. *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* CETS No. 108, COUNCIL OF EUR. (Jan. 28, 1981), www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.
153. [Criminal Code of the Russian Federation], 1996, art. 137, *translation at* www.legislationline.org/documents/section/criminal-codes/country/7.
154. *Id.*
155. *See id.*
156. Loi 80-538 du 16 juillet 1980, Relative a la communication de documents ou renseignements d'ordre economique, commercial ou technique a des personnes physiques ou morales etrangeres, JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.][OFFICIAL GAZETTE OF FRANCE], July 17, 1980, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000515863.
157. *Id.* art. 3.
158. Protection of Trading Interests Act, 1980, c. 11.
159. See Marc J. Gottridge & Thomas Rouhette, 'Blocking' Statutes Bring Discovery Woes, N.Y.L.J. (Apr. 30, 2008), <https://www.law.com/almID/900005634407/>.
160. Art. 41 PIPL, *translation at* <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>.
161. *Id.*
162. See, e.g., *Owen v. Elastos Found.*, 2023 U.S. Dist. LEXIS 6288, at *33 (S.D.N.Y. Jan. 11, 2023) (concluding “that there is no true conflict between Chinese law and defendants’ U.S. discovery obligations”); *Philips Med. Sys. (Cleveland), Inc. v. Buan*, 2022 U.S. Dist. LEXIS 35635, at *21–22 (N.D. Ill. Mar. 1, 2022) (“Defendants’ ‘understanding’ of the DSL would give the Chinese Supreme People’s Court broad power to delay or prevent discovery in American courts.”).
163. See *Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for the S. Dist. of Iowa*, 482 U.S. 522, 544 n.28 (1987); *In re Glob. Power Equip. Grp., Inc.*, 418 B.R. 833, 847 (Bankr. D. Del. 2009).
164. *In re Glob. Power Equip. Grp., Inc.*, 418 B.R. at 850.
165. *Id.* at 839, 848–49.
166. *Id.* at 848–50.
167. A recent example of the SEC’s global reach was seen in December 2020, when the SEC charged a China-based company, Luckin Coffee Inc., with intentionally fabricating revenue, expenses, and net operating losses in publicly disclosed financial statements. See Press Release, SEC, Luckin Coffee Agrees to Pay \$180 Million Penalty to Settle Accounting Fraud Charges (Dec. 16, 2020), <https://www.sec.gov/news/press-release/2020-319>. The Director of the SEC’s Division of

Enforcement explained that: “Public issuers who access our markets, regardless of where they are located, must not provide false or misleading information to investors. While there are challenges in our ability to effectively hold foreign issuers . . . accountable to the same extent as U.S. issuers and persons, we will continue to use all our available resources to protect investors when foreign issuers violate the federal securities laws.” *Id.* Luckin agreed to a settlement including a \$180 million penalty. *Id.*

168. Both DOJ and U.K. Serious Fraud Office (SFO) policy dictate that regulators cooperate where possible and consider parallel foreign investigations when determining the resolution of investigations. *See* U.S. DEP’T OF JUSTICE, JUSTICE MANUAL § 1-12.100 (2018), <https://www.justice.gov/jm/jm-1-12000-coordination-parallel-criminal-civil-regulatory-and-administrative-proceedings>; Serious Fraud Office (SFO), *Deferred Prosecution Agreements* (2020), www.sfo.gov.uk/publications/guidance-policy-and-protocols/guidance-for-corporates/deferred-prosecution-agreements-2/.

169. Press Release, U.K., *Financial Services Bill Receives Royal Assent* (Dec. 19, 2012), www.gov.uk/government/news/financial-services-bill-receives-royal-assent.

170. *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime* (Oct. 3, 2019), <https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019>.

171. Libor is defined as the rate at which a bank could borrow funds, were it to ask for and then accept interbank offers in the London market. *See* Sara Schaefer Muñoz & Max Colchester, *Barclay’s Agius is Stepping Down*, WALL ST. J. (July 1, 2012), www.wsj.com/articles/SB10001424052702304299704577500982100334286. Financial institutions use Libor as a benchmark for, among other things, floating rate loans. *See id.* Although estimates vary, during the relevant period, Libor served as the benchmark for \$10 trillion in loans to consumers and companies and for another \$350 trillion in derivatives. *See id.*

172. *See* Lindsay Fortado & Kitty Donaldson, *U.S. Libor Probers Said to Seek London Trader Interviews*, BLOOMBERG (Sept. 27, 2012), <https://www.bloomberg.com/news/articles/2012-09-27/u-s-libor-probers-said-to-seek-london-trader-interviews>.

173. *See* Carrick Mollenkamp & Mark Whitehouse, *Study Casts Doubt on Key Rate*, WALL ST. J. (May 29, 2008), <https://www.wsj.com/articles/SB121200703762027135>.

174. Jean Eaglesham & David Enrich, *Libor Probe Expands to Bank Traders*, WALL ST. J. (July 24, 2012), <https://www.wsj.com/articles/SB10000872396390443295404577545350903902004>.

175. Max Colchester & Jean Eaglesham, *Barclays Settles Rates Probe*, WALL ST. J. (June 27, 2012), <https://www.wsj.com/articles/SB10001424052702303649504577492400127596634>.

176. *See id.*
177. *See* Press Release, DOJ, No. 12-815, Barclays Bank PLC Admits Misconduct Related to Submissions for the London Interbank Offered Rate and the Euro Interbank Offered Rate and Agrees to Pay \$160 Million Penalty (June 27, 2012), <https://www.justice.gov/opa/pr/barclays-bank-plc-admits-misconduct-related-submissions-london-interbank-offered-rate-and>.
178. *See id.*
179. *United States v. Allen*, 864 F.3d 63 (2d Cir. 2017).
180. *Id.* at 100–01.
181. *Id.* at 68, 101.
182. *Kastigar v. United States*, 406 U.S. 441 (1972).
183. *Allen*, 864 F.3d at 97.
184. *See* Press Release, CFTC, No. 6737-13, CFTC Files and Settles Charges Against JPMorgan Chase Bank, N.A., for Violating Prohibition on Manipulative Conduct in Connection with “London Whale” Swaps Trades (Oct. 16, 2013) [hereinafter CFTC], www.cftc.gov/PressRoom/PressReleases/pr6737-13.
185. *See id.*
186. *See id.*
187. JPMorgan Chase & Co., Report of JPMorgan Chase & Co. Management Task Force Regarding 2012 CIO Losses 34 (Jan. 16, 2013) [hereinafter JPMorgan Chase & Co.].
188. *See id.* at 35.
189. *See id.* at 35–36.
190. *See* CFTC, *supra* note 184.
191. Ben Protesch & Raphael Minder, *Former JPMorgan Trader Surrenders in Spain in ‘London Whale’ Case*, N.Y. TIMES: DEALBOOK (Aug. 27, 2013), http://dealbook.nytimes.com/2013/08/27/spanish-authorities-arrest-former-jpmorgan-employee/?_r=0.
192. JPMorgan Chase & Co., *supra* note 187, at 7.
193. Robin Sidel, Scott Patterson & Jean Eaglesham, *J.P. Morgan Faces a Hard-Line SEC*, WALL ST. J. (Sept. 19, 2013), www.wsj.com/articles/SB10001424127887324807704579084912809151456.
194. *See id.*
195. Scott Patterson, *J.P. Morgan to Pay \$100 Million in CFTC Pact on ‘Whale’ Trades*, WALL ST. J. (Oct. 15, 2013), www.wsj.com/articles/SB10001424052702304561004579137992954471608.
196. *See id.*
197. JPMorgan Chase Bank, N.A., 2013 WL 6057042, at *9 (CFTC Oct. 16, 2013).
198. *See id.*
199. CFTC, *supra* note 184.
200. *Id.*
201. *Id.*
202. Pub. L. No. 116-222, 134 Stat. 1063 (Dec. 18, 2020).

203. See Holding Foreign Companies Accountable Act, SEC (last modified Jan. 9, 2023), <https://www.sec.gov/hfcaa>.
204. SEC v. Scoville, 913 F.3d 1204 (10th Cir. 2019).
205. Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247 (2010).
206. *Scoville*, 913 F.3d at 1218.
207. *Id.* at 1219.
208. See, e.g., Schoenbaum v. Firstbrook, 405 F.2d 200, 208 (2d Cir. 1968) (holding that a Canadian corporation's sales of treasury shares, which were only sold in Canada, met the conduct-and-effects test because those sales would affect the price of the same corporation's common-share sales in the United States).
209. Gibson Dunn, 2016 Year-End FCPA Update, (Jan. 3, 2017), www.gibsondunn.com/publications/Pages/2016-Year-End-FCPA-Update.aspx.
210. See *id.*
211. Press Release, DOJ, No. 13-613, French Oil and Gas Company, Total, S.A., Charged in the United States and France in Connection with an International Bribery Scheme (May 29, 2013), www.justice.gov/opa/pr/2013/May/13-crm-613.html.
212. Press Release, DOJ, No. 14-1448, Alstom Pleads Guilty and Agrees to Pay \$772 Million Criminal Penalty to Resolve Foreign Bribery Charges (Dec. 22, 2014), www.justice.gov/opa/pr/alstom-pleads-guilty-and-agrees-pay-772-million-criminal-penalty-resolve-foreign-bribery.
213. Press Release, SEC No. 2022-206, SEC Announces Enforcement Results for FY22 (Nov. 15, 2022), <https://www.sec.gov/news/press-release/2022-206>.
214. See *id.*
215. Remarks as Prepared for Delivery, DOJ, Acting Principal Deputy Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the 39th International Conference on the Foreign Corrupt Practices Act (Dec. 1, 2022), <https://www.justice.gov/opa/speech/acting-principal-deputy-assistant-attorney-general-nicole-m-argentieri-delivers-remarks>.
216. See *id.*
217. *Id.*
218. See *id.*
219. Press Release, SEC, No. 2016-277, Teva Pharmaceutical Paying \$519 Million to Settle FCPA Charges (Dec. 22, 2016), www.sec.gov/news/pressrelease/2016-277.html.
220. See *id.*
221. *Id.*
222. Press Release, DOJ, No. 16-1515, Odebrecht and Braskem Plead Guilty and Agree to Pay at Least \$3.5 Billion in Global Penalties to Resolve Largest Foreign Bribery Case in History (Dec. 21, 2016), www.justice.gov/opa/pr/odebrecht-and-braskem-plead-guilty-and-agree-pay-least-35-billion-global-penalties-resolve.
223. Gibson Dunn, *supra* note 209.
224. See *id.*

SEC COMPLIANCE AND ENFORCEMENT AB 2023

225. *Id.*
226. SEC v. Cohen, 332 F. Supp. 3d 575 (E.D.N.Y. 2018).
227. *Id.* (citing SEC v. Kokesh, 137 S. Ct. 1635 (2017)).
228. *See id.* at 589–91, 594 (noting that tolling agreements are legally ineffective unless the allegedly corrupt activity purportedly subject to tolling is clearly within the scope of a tolling provision).
229. United States v. Hoskins, 902 F.3d 69 (2d Cir. 2018).
230. *Id.* at 94.
231. United States v. Hoskins, 3:12-cr-99238-JBA, 2020 WL 914302 (D. Conn. Feb. 26, 2020).
232. Under well-settled agency law, a principal cannot be liable for its agent’s tortious conduct if the agent itself is not liable. *See, e.g.,* Crawford v. Signet Bank, 179 F.3d 926, 929 (D.C. Cir. 1999). The logical extension of this would be that a principal cannot be liable under the FCPA for its agent’s conduct if the agent itself cannot be held liable per *Hoskins*.
233. U.S. DEP’T OF JUSTICE, JUSTICE MANUAL § 9-47.120 (2018), www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#9-47.120.
234. *Id.*
235. Press Release, DOJ, No. 18-975, Deputy Assistant Attorney General Matthew S. Miner, Remarks at the American Conference Institute 9th Global Forum on Anti-Corruption Compliance in High Risk Markets (July 25, 2018), www.justice.gov/opa/pr/deputy-assistant-attorney-general-matthew-s-miner-remarks-american-conference-institute-9th.
236. Memorandum from Brian A. Benczkowski, Assistant Attorney Gen., DOJ, to All Criminal Division Personnel, Selection of Monitors in Criminal Division Matters (Oct. 11, 2018), www.justice.gov/opa/speech/file/1100531/download.
237. Rod J. Rosenstein, Deputy Attorney Gen., DOJ, Remarks at the American Conference Institute’s 35th International Conference on the Foreign Corrupt Practices Act (Nov. 29, 2018), www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0.
238. *Id.*
239. A Resource Guide to the U.S. Foreign Corrupt Practices Act, by the Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission (updated July 2020), <https://www.justice.gov/criminal-fraud/fcpa-guidance>.
240. *Id.* at 36.
241. Press Release, DOJ, No. 13-975, United States and Switzerland Issue Joint Statement Regarding Tax Evasion Investigations (Aug. 29, 2013), www.justice.gov/opa/pr/united-states-and-switzerland-issue-joint-statement-regarding-tax-evasion-investigations.
242. Lynnley Browning & Julia Werdigier, *Switzerland to Allow Its Banks to Disclose Hidden Client Accounts*, N.Y. TIMES: DEALBOOK (May 29, 2013), <http://dealbook.nytimes.com/2013/05/29/swiss-officials-to-allow-banks-to-sidestep-secrecy-laws/>.

243. Press Release, DOJ, No. 16-093, Justice Department Announced Final Swiss Bank Program Category 2 Resolution with HSZH Verwaltungs AG (Jan. 27, 2016), www.justice.gov/opa/pr/justice-department-announces-final-swiss-bank-program-category-2-resolution-hszh-verwaltungs.

244. See IRS, Criminal Investigation, Joint Chiefs of Global Tax Enforcement, <https://www.irs.gov/compliance/joint-chiefs-of-global-tax-enforcement#:~:text=The%20J5%20was%20formed%20in,countries%20and%20organisations%20where%20appropriate>.

245. See *id.*

246. See IRS, Joint Chiefs of Global Tax Enforcement Successes (July 7, 2020), <https://www.irs.gov/pub/foia/ig/ci/j5-one-pager-07-14-2020.pdf>.

Appendix 12A

Current Signatories of the IOSCO MOU

The following are the current signatories of the IOSCO MOU (as of January 2023).*

	Member Agency	Jurisdiction	Date of Formal Signing
1	Financial Services Regulatory Authority (FSRA)	Abu Dhabi	Jan. 15, 2017
2	Astana Financial Services Authority (AFSA)	AIFC, Nur-Sultan (formerly Astana)	July 3, 2019
3	Albanian Financial Supervisory Authority (AFSA)	Albania	June 23, 2009
4	Alberta Securities Commission (ASC)	Alberta	Nov. 10, 2003
5	Commission d'Organisation et de Surveillance des Opérations de Bourse (COSOB)	Algeria	May 8, 2019
6	Autoritat Financera Andorrana (AFA)	Andorra	Sept. 18, 2013

* See www.iosco.org/about/?subSection=mmou&subSection1=signatories.

App. 12A-1

	Member Agency	Jurisdiction	Date of Formal Signing
7	Comissão do Mercado de Capitais (CMC)	Angola	July 12, 2017
8	Comisión Nacional de Valores (CNV)	Argentina	June 12, 2014
9	Central Bank of Armenia (CBA)	Armenia	Jan. 18, 2018
10	Australian Securities and Investments Commission (ASIC)	Australia	Oct. 8, 2002
11	Financial Market Authority (FMA)	Austria	Oct. 28, 2009
12	Securities Commission of The Bahamas (SCB)	Bahamas	Dec. 27, 2012
13	Central Bank of Bahrain (CBB)	Bahrain, Kingdom of	Feb. 12, 2008
14	Bangladesh Securities and Exchange Commission (BSEC)	Bangladesh	Dec. 22, 2013
15	Financial Services and Markets Authority (FSMA) <i>Formerly: Banking, Finance and Insurance Commission (BFIC)</i>	Belgium	Apr. 3, 2005
16	Bermuda Monetary Authority (BMA)	Bermuda	June 7, 2007
17	Securities Commission of the Federation of Bosnia and Herzegovina (SCFBH)	Bosnia and Herzegovina, Federation of	Oct. 12, 2012
18	Comissão de Valores Mobiliários (CVM)	Brazil	Oct. 21, 2009
19	British Columbia Securities Commission (BCSC)	British Columbia	Nov. 10, 2003
20	British Virgin Islands Financial Services Commission (FSC)	British Virgin Islands	May 21, 2007
21	Brunei Darussalam Central Bank (BDCB)	Brunei	Mar. 4, 2016

App. 12A-2

	Member Agency	Jurisdiction	Date of Formal Signing
22	Financial Supervision Commission (FSC)	Bulgaria	Oct. 29, 2009
23	Auditoria Geral do Mercado de Valores Mobiliários, Banco Central of Cabo Verde (AGMVM)	Cabo Verde	May 8, 2019
24	Cayman Islands Monetary Authority (CIMA)	Cayman Islands	Mar. 24, 2009
25	Commission de Surveillance du Marché Financier de l’Afrique Centrale (Securities and Exchange Commission of Central Africa) (COSUMAF)	Central Africa	Nov. 9, 2015
26	Comisión para el Mercado Financiero (Financial Market Commission) (CMF)	Chile	Nov. 22, 2018
27	China Securities Regulatory Commission (CSRC)	China	May 29, 2007
28	Superintendencia Financiera de Colombia (SFC)	Colombia	Mar. 26, 2012
29	Superintendencia General de Valores (SGV)	Costa Rica	Apr. 19, 2022
30	Croatian Financial Services Supervisory Agency (HANFA)	Croatia, Republic of	Oct. 20, 2009
31	Cyprus Securities and Exchange Commission (CYSEC)	Cyprus	Oct. 22, 2009
32	Czech National Bank (CNB) <i>Formerly: Czech Securities Commission</i>	Czech Republic	Mar. 29, 2007
33	Danish Financial Supervisory Authority (FSA)	Denmark	Aug. 17, 2006
34	Dubai Financial Services Authority (DFSA)	DIFC, Dubai	July 3, 2006

App. 12A-3

	Member Agency	Jurisdiction	Date of Formal Signing
35	Superintendencia del Mercado de Valores (SIMV) <i>Formerly: Superintendencia de Valores, Banco Central de la República Dominicana</i>	Dominican Republic	May 3, 2018
36	Superintendencia de Compañías, Valores y Seguros (SCVS)	Ecuador	Feb. 18, 2016
37	Financial Regulatory Authority (FRA) <i>Formerly: Capital Market Authority</i>	Egypt	May 16, 2012
38	Superintendencia del Sistema Financiero (SSF)	El Salvador	Oct. 10, 2012
39	Finantsinspektsioon (FI)	Estonia	Mar. 4, 2011
40	Financial Supervision Authority (FSA)	Finland	Nov. 22, 2007
41	Autorité des marchés financiers (AMF) <i>Formerly: Commission des Opérations de Bourse (COB)</i>	France	Feb. 19, 2003
42	National Bank Of Georgia (NBG)	Georgia	Aug. 10, 2021
43	Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)	Germany	Nov. 5, 2003
44	Securities and Exchange Commission (SEC)	Ghana	Sept. 19, 2022
45	Gibraltar Financial Services Commission (GFSC)	Gibraltar	Dec. 20, 2013
46	Hellenic Capital Market Commission (HCMC)	Greece	Oct. 18, 2002
47	Guernsey Financial Services Commission (GFSC)	Guernsey	Feb. 25, 2009
48	Securities and Futures Commission (SFC)	Hong Kong	Mar. 3, 2003

App. 12A-4

	Member Agency	Jurisdiction	Date of Formal Signing
49	Magyar Nemzeti Bank (The Central Bank of Hungary) (MNB)	Hungary	July 9, 2003
50	The Central Bank of Iceland (CBI)	Iceland	June 23, 2010
51	International Financial Services Centres Authority (IFSCA)	India	Aug. 3, 2022
52	Securities and Exchange Board of India (SEBI)	India	Apr. 22, 2003
53	Indonesia Financial Services Authority (OJK)	Indonesia	Jan. 21, 2014
54	Securities and Exchange Organization (SEO)	Iran	Nov. 27, 2018
55	Central Bank of Ireland (CBI) <i>Formerly: Central Bank and Financial Services Authority of Ireland (CBFSAI)</i>	Ireland	Dec. 24, 2012
56	Isle of Man Financial Services Authority (IOMFSA)	Isle of Man	Oct. 21, 2005
57	Israel Securities Authority (ISA)	Israel	July 2, 2006
58	Commissione Nazionale per le Società e la Borsa (CONSOB)	Italy	Sept. 15, 2003
59	Financial Services Commission (JFSC)	Jamaica	Feb. 13, 2015
60	Financial Services Agency (FSA)	Japan	Feb. 19, 2008
61	Ministry of Agriculture, Forestry and Fisheries (MAFF)	Japan	May 9, 2011
62	Ministry of Economy, Trade and Industry (METI)	Japan	May 9, 2011
63	Jersey Financial Services Commission (FSC)	Jersey	Mar. 6, 2003
64	Jordan Securities Commission (JSC)	Jordan	Feb. 13, 2008

App. 12A-5

	Member Agency	Jurisdiction	Date of Formal Signing
65	Agency of the Republic of Kazakhstan for Regulation and Development of Financial Market (ARDFM)	Kazakhstan, Republic of	Nov. 27, 2018
66	Capital Markets Authority (CMA)	Kenya	Feb. 27, 2009
67	Financial Services Commission/ Financial Supervisory Service (FSC/FSS)	Korea, Republic of	June 9, 2010
68	Capital Markets Authority (CMA)	Kuwait	May 15, 2017
69	Labuan Financial Services Authority (FSA)	Labuan	May 16, 2012
70	Financial and Capital Market Commission (FCMC)	Latvia, Republic of	Feb. 18, 2013
71	Financial Market Authority (FMA)	Liechtenstein	Apr. 20, 2011
72	Bank of Lithuania (BL) <i>Formerly: Lithuanian Securities Commission</i>	Lithuania	July 15, 2003
73	Commission de Surveillance du Secteur Financier (CSSF)	Luxembourg	May 8, 2007
74	Reserve Bank of Malawi (RBM)	Malawi	Mar. 13, 2013
75	Securities Commission (SC)	Malaysia	May 7, 2007
76	Capital Market Development Authority (CMDA)	Maldives	Oct. 29, 2009
77	Malta Financial Services Authority (MFSA)	Malta	Mar. 9, 2006
78	Financial Services Commission (FSC)	Mauritius	May 16, 2012
79	Comisión Nacional Bancaria y de Valores (CNBV)	Mexico	Mar. 14, 2003
80	Commission de Contrôle des Activités Financières (CCAF)	Monaco, Principality of	Sept. 26, 2022
81	Financial Regulatory Commission (FRC)	Mongolia	June 18, 2014

App. 12A-6

	Member Agency	Jurisdiction	Date of Formal Signing
82	Capital Market Authority of Montenegro (CMA)	Montenegro	Feb. 25, 2009
83	Autorité Marocaine du Marché des Capitaux (AMMC)	Morocco	Dec. 10, 2007
84	The Dutch Authority for the Financial Markets (AFM) <i>Formerly: Stichting Toezicht Effectenverkeer</i>	The Netherlands	Nov. 22, 2007
85	Financial Markets Authority (FMA) <i>Formerly: Securities Commission (SC)</i>	New Zealand	Dec. 1, 2003
86	Securities and Exchange Commission (SEC)	Nigeria	June 8, 2006
87	Securities and Exchange Commission of the Republic of North Macedonia (SEC)	North Macedonia, Republic of	Oct. 18, 2010
88	Finanstilsynet (The Financial Supervisory Authority of Norway) (FSA)	Norway	Dec. 11, 2006
89	Capital Market Authority (CMA)	Oman, Sultanate of	Mar. 24, 2012
90	Ontario Securities Commission (OSC)	Ontario	Oct. 23, 2002
91	Securities and Exchange Commission (SECP)	Pakistan	Mar. 10, 2011
92	Palestine Capital Market Authority (PCMA)	Palestine	Feb. 21, 2014
93	Superintendencia del Mercado de Valores (SMV)	Panama	May 16, 2017
94	Superintendencia del Mercado de Valores (SMV) <i>Formerly: Comisión Nacional Supervisora de Empresas y Valores (CONASEV)</i>	Peru	May 16, 2012

App. 12A-7

	Member Agency	Jurisdiction	Date of Formal Signing
95	Polish Financial Supervision Authority (UKNF) <i>Formerly: Polish Securities and Exchange Commission</i>	Poland	Nov. 4, 2003
96	Comissão do Mercado de Valores Mobiliários (CMVM)	Portugal	Nov. 4, 2002
97	Qatar Financial Centre Regulatory Authority (QFCRA)	Qatar	Jan. 15, 2017
98	Qatar Financial Markets Authority (QFMA)	Qatar	Feb. 27, 2013
99	Autorité des marchés financiers (AMF)	Quebec	Dec. 17, 2002
100	Financial Supervisory Authority (ASF)	Romania	Nov. 4, 2008
101	The Bank of Russia (CBR)**	Russia	Feb. 16, 2015
102	Capital Market Authority (CMA)	Saudi Arabia	June 9, 2010
103	Securities Commission (SC)	Serbia, Republic of	Oct. 29, 2009
104	Monetary Authority of Singapore (MAS)	Singapore	Nov. 17, 2005
105	The National Bank of Slovakia (NBS) <i>Formerly: Financial Market Authority</i>	Slovak Republic	June 17, 2004
106	Securities Market Agency/Agencija Za Trg Vrednostnih Papirjev (SMA)	Slovenia	Oct. 20, 2009
107	Financial Sector Conduct Authority (FSCA)	South Africa	Mar. 18, 2003
108	Comisión Nacional del Mercado de Valores (CNMV)	Spain	Mar. 24, 2003
109	Securities and Exchange Commission of Sri Lanka (SEC)	Sri Lanka	Mar. 31, 2004

** Not an active member.

App. 12A-8

	Member Agency	Jurisdiction	Date of Formal Signing
110	Securities Commission of the Republic Srpska (SECRS)	Srpska, Republic of	Oct. 27, 2009
111	Finansinspektionen (FI)	Sweden	May 17, 2011
112	Swiss Financial Market Supervisory Authority (FINMA) <i>Formerly: Swiss Federal Banking Commission (Commission fédérale des banques)</i>	Switzerland	Feb. 15, 2010
113	Syrian Commission on Financial Markets and Securities (SCFMS)	Syria	June 9, 2010
114	Financial Supervisory Commission (FSC)	Chinese Taipei	Mar. 15, 2011
115	Capital Markets and Securities Authority (CMSA)	Tanzania	Apr. 18, 2011
116	Securities and Exchange Commission (SEC)	Thailand	June 19, 2008
117	Trinidad and Tobago Securities and Exchange Commission (TTSEC)	Trinidad and Tobago	June 19, 2013
118	Conseil du marché financier (CMF)	Tunisia	Dec. 25, 2009
119	Capital Markets Board (CMB)	Türkiye	Nov. 14, 2002
120	Turks & Caicos Islands Financial Services Commission (TCIFSC)	Turks & Caicos	Mar. 24, 2016
121	Capital Markets Authority (CMA)	Uganda	Jan. 16, 2017
122	Securities and Commodities Authority (SCA)	United Arab Emirates	Oct. 11, 2012
123	Financial Conduct Authority (FCA) <i>Formerly: Financial Services Authority</i>	United Kingdom	Mar. 10, 2003
124	Commodity Futures Trading Commission (CFTC)	United States of America	Dec. 19, 2002

App. 12A-9

	Member Agency	Jurisdiction	Date of Formal Signing
125	Securities and Exchange Commission (SEC)	United States of America	Nov. 19, 2002
126	Banco Central del Uruguay (BCU)	Uruguay	June 9, 2010
127	State Securities Commission (SSC)	Vietnam	Sept. 18, 2013
128	Conseil régional de l'épargne publique et des marchés financiers (CREPMF)	West African Monetary Union	June 25, 2009
129	Securities and Exchange Commission (SEC)	Zambia	Jan. 15, 2018

App. 12A-10