

The Sedona Conference Draft Commentary on the Enforceability in U.S. Court of Orders and Judgments Entered Under GDPR (June 2019)



Copyright 2019, The Sedona Conference.
All rights reserved.

Draft Commentary on the Enforceability in U.S. Courts of Orders and Judgments Entered Under GDPR (June 2019)

Drafting Team:

Alex Pearce (Drafting Team Leader)

Joseph Dickinson

Starr Drum

Marcel Duhamel

Ron Hedges

Eric Mandel

Shoshana Rosenberg

Meredith Schultz

David Shonka

Claire Spencer

Bob Cattnach (Steering Committee Liaison)

Draft Commentary on the Enforceability in U.S. Courts of Orders and Judgments Entered Under GDPR

Table of Contents

Introduction.....	1
I. Background and General Governing Principles.....	2
A. The applicable substantive law	3
B. Foundational requirements for recognition and enforcement of foreign judgments	4
C. The rule against recognition of foreign fines and penal judgments.....	5
D. Other grounds for nonrecognition of foreign judgments	6
E. Recognition of foreign administrative orders	7
F. Procedural considerations and burdens of proof.....	8
II. Recognition and Enforcement of GDPR Orders and Judgments in U.S. Courts— Considerations for Private Plaintiffs.....	8
A. General considerations for private causes of action	9
B. Data subject compensation claims under GDPR Article 82	11
1. Overview and general considerations	11
2. Enforceability under U.S. law.....	12
C. Injunctions and non-monetary orders issued under GDPR Article 79	13
1. Overview and general considerations	13
2. Enforceability under U.S. law.....	13
III. Recognition and Enforcement of GDPR Orders and Judgments in U.S. Courts— Considerations for EU Supervisory Authorities	14
A. Overview and general considerations	14
B. Non-monetary orders issued under Article 58: enforceability under U.S. law.....	16
C. Administrative fines issued under Articles 58.2(i) and 83: enforceability under U.S. law.....	17
IV. Recognition and Enforcement of GDPR Orders and Judgments in U.S. Courts— Considerations for U.S.-based Organizations	18
A. Overview and general considerations	18
1. Application of GDPR under Article 3.1	18
2. Application of GDPR under Article 3.2	19

3.	Application of GDPR Under Article 28.....	21
4.	General Considerations	21
B.	Key defenses to a recognition action	22
1.	Lack of personal jurisdiction over the defendant in the EU	22
a.	Personal jurisdiction under GDPR Article 3.1	25
b.	Personal jurisdiction under Article 3.2	26
c.	DPOs and Article 27 representatives: impact on personal jurisdiction in the EU	27
2.	Repugnancy to federal or state public policy.....	28
V.	Alternative Routes to GDPR Enforcement in U.S. Courts: The Federal Trade Commission, Privacy Shield, and Contract Claims	29
A.	The Federal Trade Commission and Privacy Shield remedies	30
B.	Contract actions associated with data protection	31
1.	Contracts between data subjects and data controllers.....	31
2.	Contracts between data controllers and data processors.....	32
3.	Contracts related to employment or engagement of DPOs and EU representatives.....	33

Introduction

This Commentary evaluates the enforceability in a U.S. court of an order or judgment entered under the European Union (“EU”) General Data Protection Regulation (“GDPR”)¹ by an EU court, or by an EU Member State supervisory authority, against a U.S.-based controller or processor. The goal of the Commentary is to provide guidance to stakeholders in the EU and the broader European Economic Area,² as well as in the U.S., on the factors—both legal and practical—that speak to whether and how such an order or judgment could be enforced through resort to the U.S. judicial system.

GDPR represents a significantly expanded territorial reach over its predecessor, the Data Protection Directive. GDPR Article 3 establishes two primary groups of entities that must comply. Under GDPR Article 3.1 the law applies to the processing of personal data in the context of an establishment of a controller or processor in the EU, regardless of where the processing takes place.³ Thus, for example, if a multinational company possesses anyone’s personal data (either directly from the person him or herself, or by buying it) and the data relates to the business of the company’s EU offices, that data is subject to GDPR.⁴ Article 3.2 is even broader in its extraterritorial claims. It says that a controller or processor with no physical presence in the EU is still subject to GDPR if it offers goods or services to people “in” the EU or if it otherwise monitors the behavior of people when they are in the EU.⁵ A third category of companies can also be subject to GDPR’s requirements—companies that do not fall within the territorial scope of Article 3, but process personal data on behalf of companies that do fall within Article 3’s purview.⁶

The Commentary does not take issue with GDPR’s extraterritorial aspirations or seek to define the precise contours of its extraterritorial reach. There are plenty of examples where U.S.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1).

² GDPR has been incorporated into the European Economic Area (EEA) Agreement by the EEA Joint Committee, and thus applies to all Member States of the EEA, i.e., Member States of the EU (currently Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Ireland, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Spain, Slovakia, Slovenia, Sweden and, until March 29, 2019, the United Kingdom), plus Iceland, Liechtenstein and Norway (note: Switzerland has not ratified the EEA Agreement, and GDPR has no direct application). See, *General Data Protection Regulation incorporated into the EEA Agreement*, European Free Trade Association, 6 July 2018, available at <https://www.efta.int/EEA/news/General-Data-Protection-Regulation-incorporated-EEA-Agreement-509291>. Thus, for simplicity’s sake, this Commentary will use the term “EU” to refer to all Member States of the EEA.

³ GDPR art. 3.1.

⁴ In this regard, it is important to note that GDPR defines “processing” to include virtually any use of personal data, including “collection,” “recording,” “storage,” “consultation,” and “making available.” GDPR art. 4(2). Additionally, “personal data” is broadly defined to mean “any information related to an identified or identifiable natural person.”

⁵ GDPR art. 3.2.

⁶ See GDPR art. 28.1.

courts or agencies have asserted that U.S. laws have extraterritorial effect,⁷ and so we will assume that the EU can make the same claim with respect to its laws. We leave the validity of the extraterritorial claims for someone else to address. Suffice it to say that under GDPR, it is foreseeable that EU courts and supervisory authorities will exercise their authority to enter orders and obtain judgments—through proceedings that take place in the EU under the laws of its Member States—against U.S. organizations.

This Commentary will address what happens *after* an order or judgment has been entered in the EU. It will evaluate the options for a party in the EU—whether a supervisory authority, individual data subject, or a not-for-profit body acting on behalf of data subjects—to obtain a U.S.-based organization’s compliance through resort to a proceeding in a U.S. court.

To that end, we intend the Commentary to be useful both to GDPR experts and those less familiar with GDPR, to help them understand how and under what circumstances GDPR orders and judgments might be enforceable under U.S. law. The Commentary is drafted to be useful to people on both sides of the Atlantic—to those in the EU who wonder whether and how they might obtain relief from a company in the U.S. for violations of GDPR, as well as those in the U.S. who might wonder whether and how GDPR’s extraterritorial scope will be recognized by a U.S. court.

Part I of the Commentary will provide a brief overview of the state of the law in the U.S. regarding the recognition and enforcement of foreign country orders and judgments. It should not be a surprise to anyone that over the past 230 years, the issue has been raised and addressed many times. While some states have addressed it by adopting statutes, and others have relied on the common law, each approach relies on a set of common principles. Part I will describe those principles, touching on questions about enforcement of private money judgments and injunctions as well as public orders prohibiting or mandating certain conduct or levying fines or other penalties for violations of foreign laws.

Building on that discussion of general principles, Parts II, III, and IV will next address the factors—both practical and legal—that three constituencies should consider when evaluating the enforceability of a GDPR order or judgment in a U.S. court: private plaintiffs in the EU (Part II), EU supervisory authorities (Part III), and U.S.-based organizations (Part IV).

Finally, Part V will briefly address the ways that GDPR’s requirements might be enforced through U.S. courts other than through the direct enforcement of an existing EU order or judgment entered under GDPR, including by the U.S. Federal Trade Commission and individual data subjects under the EU-U.S. Privacy Shield and through contract-based claims arising from GDPR-related agreements.

I. Background and General Governing Principles

⁷ See, e.g., Department of Justice and Federal Trade Commission Antitrust Guidelines for International Enforcement and Cooperation at 16-36 (and cases cited therein) (January 13, 2017), available at <https://www.justice.gov/atr/internationalguidelines/download>.

This Part of the Commentary summarizes the general principles under existing U.S. law that govern the recognition and enforcement of foreign country orders and judgments. It is not intended to be a comprehensive primer on the law in this area. Rather, its purpose is to identify and briefly summarize those principles that are most relevant to the enforceability of a judgment or order entered in the EU under GDPR.

A. The applicable substantive law

The question of recognition and enforcement of foreign judgments and orders arises from the foundational principle that under U.S. law, any judgment from a country or U.S. state outside a given forum is considered “foreign” and cannot be directly enforced in that forum without a legal basis to “recognize” the judgment domestically.⁸ The Full Faith and Credit Clause in Article IV of the Constitution provides that legal basis for judgments rendered in any other court—state or federal—in the United States.⁹

The Full Faith and Credit Clause does not apply, however, to judgments rendered by courts in foreign countries. Nor is there any U.S. federal statute or treaty dealing generally with foreign country judgment recognition. Instead, recognition of foreign country judgments is primarily a matter of state law, and its historical roots can be traced back to the U.S. Supreme Court’s 1895 decision in *Hilton v. Guyot*.¹⁰

In *Hilton*, the U.S. Supreme Court concluded that in the absence of a treaty, U.S. courts asked to recognize a foreign judgment should turn to the principle of comity, which the court explained is “neither a matter of absolute obligation . . . nor a mere courtesy and good will,” but rather “the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws.”¹¹ After reviewing the leading authorities on the subject at the time, the *Hilton* court set forth the following considerations that would justify recognizing the judgment of a foreign court:

[W]here there has been opportunity for a full and fair trial abroad before a court of competent jurisdiction, conducting the trial upon regular proceedings, after due citation or voluntary appearance of the defendant, and under a system of jurisprudence likely to secure an impartial administration of justice between the citizens of its own country and those of other countries, and there is nothing to show either prejudice in the court, or in the system of laws under which it was sitting, or fraud in procuring the judgment, or any other special reason why the comity of this

⁸ Yuliya Zeynalova, *The Law on Recognition and Enforcement of Foreign Judgments: Is It Broken and How Do We Fix It?*, 31 BERKELEY J. INT’L L. 150, 154 (2013).

⁹ See U.S. Const. art. IV, § 1.

¹⁰ Ronald A. Brand, *Federal Judicial Center International Litigation Guide: Recognition and Enforcement of Foreign Judgments*, 74 U. PITT. L. REV. 491, 496 (2013) (citing *Hilton v. Guyot*, 159 U.S. 113 (1895)).

¹¹ *Hilton*, 159 U.S. at 163-164.

nation should not allow it full effect, the merits of the case should not, in an action brought in this country upon the judgment, be tried afresh.¹²

Using *Hilton* as a conceptual backdrop, states generally follow one of two approaches to recognizing foreign country judgments: (1) recognition at common law as a matter of comity; or (2) recognition under state statutes that are based on one of two model acts promulgated by the Uniform Law Commission.¹³

Courts in a minority of states—sixteen—follow the first approach.¹⁴ They generally rely on *Hilton*, the Restatement (Third) of Foreign Relations Law¹⁵ (recently succeeded by the Restatement (Fourth) of Foreign Relations Law¹⁶) and the Restatement (Second) of Conflict of Laws.¹⁷

Courts in the other thirty-four states have adopted one of two model recognition acts:¹⁸ (1) the 1962 Uniform Foreign Money Judgments Recognition Act (the “1962 Recognition Act”),¹⁹ or (2) the 2005 Uniform Foreign-Country Money Judgments Recognition Act (the “2005 Recognition Act”)²⁰ (collectively, the “Recognition Acts”).

While U.S. law regarding foreign judgment recognition may thus seem to be a disparate patchwork,²¹ the common law and both Recognition Acts are largely consistent as to both the foundational requirements to recognize a foreign judgment and the primary grounds for non-recognition.

B. Foundational requirements for recognition and enforcement of foreign judgments

Under the common law and both Recognition Acts, to be recognizable by a U.S. court a foreign judgment must be (1) final, (2) conclusive, and (3) enforceable in the rendering country.²² A judgment is “final” for this purpose when it “is not subject to additional proceedings in the

¹² *Id.* at 202-03.

¹³ Tanya J. Monestier, *Whose Law of Personal Jurisdiction? The Choice of Law Problem in the Recognition of Foreign Judgments*, 96 B.U. L. REV. 1729, 1736 (2016).

¹⁴ Ronald A. Brand, *The Continuing Evolution of U.S. Judgments Recognition Law*, 55 COLUM. J. TRANSNAT'L L. 277, 295 (2017).

¹⁵ RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW (AM. LAW INST. 1987) (hereinafter “RESTATEMENT (THIRD)”).

¹⁶ RESTATEMENT (FOURTH) OF FOREIGN RELATIONS LAW (AM. LAW INST. 2018) (hereinafter “RESTATEMENT (FOURTH)”).

¹⁷ RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 98 (AM. LAW INST. 1971).

¹⁸ Brand, *supra* note 14, at 295.

¹⁹ UNIF. FOREIGN MONEY-JUDGMENTS RECOGNITION ACT (UNIF. LAW COMM'N 1962) (hereinafter 1962 RECOGNITION ACT).

²⁰ UNIF. FOREIGN-COUNTRY MONEY JUDGMENTS RECOGNITION ACT (UNIF. LAW COMM'N 2005) (hereinafter 2005 RECOGNITION ACT).

²¹ Monestier, *supra* note 13, at 1735.

²² 1962 RECOGNITION ACT § 2; 2005 RECOGNITION ACT § 3(a)(2); RESTATEMENT (THIRD) § 481; RESTATEMENT (FOURTH) § 481.

rendering court other than execution.”²³ Importantly, both contested and default judgments can meet these criteria.²⁴ While being subject to an appeal “does not deprive it of its character as a final judgment,”²⁵ a U.S. court may—but is not required to—stay the recognition of a foreign judgment until the appeal has run its course in the rendering country.²⁶

Notably, the 1962 Recognition Act and the 2005 Recognition Act are limited by their own terms to judgments that grant or deny recovery of a sum of money.²⁷ The common law approach, however, also allows for a U.S. court to *recognize* foreign judgments that grant injunctions, declare parties’ rights, or determine parties’ legal status.²⁸ Whether and under what circumstances a U.S. court will *enforce* these non-monetary judgments, however, is less clear.

The Restatement (Third) of Foreign Relations Law and the Restatement (Fourth) of Foreign Relations Law suggest that U.S. courts are *not* required to enforce these judgments by granting the relief ordered by the rendering court.²⁹

The Restatement (Second) of Conflict of Laws, by contrast, concludes that foreign injunctive decrees *can* be enforced, provided that such enforcement is “necessary to effectuate the [foreign court’s] decree and will not impose an undue burden upon the American court and provided further that in the view of the American court the decree is consistent with fundamental principles of justice and of good morals.”³⁰ At least two federal courts have relied on that statement to conclude that they could enforce injunctions entered by foreign courts under the principle of comity.³¹

C. The rule against recognition of foreign fines and penal judgments

²³ RESTATEMENT (THIRD) § 481 cmt. e. *See also* RESTATEMENT (FOURTH) § 481 cmt. d.

²⁴ *See Brand, supra* note 10, at 524 (explaining that “any decision on the merits that could have been litigated in the originating court will have preclusive effect in the recognizing court,” but noting that “this does not prevent challenges based on lack of personal jurisdiction or lack of proper notice in the originating court, or other grounds for non-recognition otherwise available under the applicable statute or common law”).

²⁵ RESTATEMENT (THIRD) § 481 cmt. e.

²⁶ 1962 RECOGNITION ACT § 6; 2005 RECOGNITION ACT § 8; RESTATEMENT (THIRD) § 481 cmt. e.; RESTATEMENT (FOURTH) § 481 cmt. e.

²⁷ 1962 RECOGNITION ACT §§ 1(2), 3; 2005 RECOGNITION ACT § 3(a)(1).

²⁸ RESTATEMENT (THIRD) § 481 cmt. b (“Judgments granting injunctions, declaring rights or determining status . . . may be entitled to recognition under this and the following sections.”); RESTATEMENT (FOURTH) § 488 (“[A] final and conclusive judgment of a court in a foreign state in an action seeking an injunction or a comparable nonmonetary remedy is entitled to recognition by courts in the United States.”); Restatement (Second) of Conflict of Laws §102 cmt. g (Am. Law Inst. 1971) (“A valid decree rendered in a foreign nation that orders or enjoins the doing of an act will usually be recognized in the United States.”).

²⁹ RESTATEMENT (THIRD) § 481 cmt. b (“Judgments granting injunctions, declaring rights or determining status . . . are not generally entitled to enforcement.”); RESTATEMENT (FOURTH) § 488 (“[T]he question of what remedies to grant as a result of recognition of the foreign judgment, including whether to provide injunctive relief, does not depend on the remedies provided by the rendering court.”).

³⁰ Restatement (Second) of Conflict of Laws §102 cmt. g (Am. Law Inst. 1971).

³¹ *See Siko Ventures Ltd. v. Argyll Equities, LLC*, No. SA-05-CA-100-OG, 2005 WL 2233205, at *3 (W.D. Tex. Aug. 5, 2005); *Pilkington Bros. P.L.C. v. AFG Indus. Inc.*, 581 F. Supp. 1039, 1043 (D. Del. 1984).

The general rule in favor of recognizing foreign country judgments that meet the foundational requirements above is subject to a key exception: under both the Recognition Acts and the common law, U.S. courts generally do not recognize or enforce foreign judgments for the collection of taxes, fines, or penalties.³²

A judgment is “penal” for purposes of this rule when it is “in favor of a foreign state or one of its subdivisions, and primarily punitive rather than compensatory in character.”³³ The rule against recognizing such judgments reflects “a reluctance of courts to subject foreign public law to judicial scrutiny . . . combined with a reluctance to enforce law that may conflict with the public policy of the forum state.”³⁴

The Recognition Acts both expressly exclude foreign fines and penal judgments from their provisions for recognition.³⁵ The 2005 Recognition Act, however, includes a savings clause that leaves room for the recognition of such judgments on other grounds, such as comity under the common law approach.³⁶

Under the Restatement (Third) of Foreign Relations Law, the common law rule against recognizing fines and penal judgments is phrased as being permissive, rather than mandatory.³⁷ As a comment explains, nonrecognition is permitted on this basis, but not required, as “no rule of United States law or of international law would be violated if a court in the United States enforced a judgment of a foreign court for payment of taxes or comparable assessments that was otherwise consistent” with the standards for recognition.³⁸

The Restatement (Fourth) of Foreign Relations Law, by contrast, simply states that courts “do not” recognize or enforce foreign judgments “to the extent such judgments are for taxes, fines, or other penalties, unless authorized by a statute or an international agreement.”³⁹

D. Other grounds for nonrecognition of foreign judgments

Assuming a foreign judgment meets the foundational requirements above and is not subject to nonrecognition as a fine or penalty, both the common law approach and the Recognition Acts provide several other grounds for nonrecognition.

³² See RESTATEMENT (THIRD) § 483; RESTATEMENT (FOURTH) § 489; 1962 RECOGNITION ACT § 1(2); 2005 RECOGNITION ACT § 3(b).

³³ RESTATEMENT (THIRD) § 483 cmt. b. See also RESTATEMENT (FOURTH) § 489 cmt. b.

³⁴ RESTATEMENT (THIRD) § 483 reporter’s note 2.

³⁵ 1962 RECOGNITION ACT § 1(2) (defining “foreign judgment” that is subject to recognition as excluding “a judgment for taxes, a fine, or other penalty”); 2005 RECOGNITION ACT § 3(b) (providing that the act does not apply “to the extent that the judgment is . . . a fine or other penalty”).

³⁶ 2005 RECOGNITION ACT § 11 (“This act does not prevent the recognition under principles of comity or otherwise of a foreign-country judgment not within the scope of this act.”).

³⁷ RESTATEMENT (THIRD) § 483 (“Courts in the United States are not required to enforce [penal judgments].”).

³⁸ *Id.* § 483 cmt. a.

³⁹ RESTATEMENT (FOURTH) § 489.

Some of these grounds are mandatory. A U.S. court cannot enforce a foreign judgment, for example, if the rendering court lacked personal jurisdiction over the defendant.⁴⁰ There is some question as to whose law governs the U.S. court's determination of that issue: the law of the rendering country, the law of the U.S. forum, or some combination thereof.⁴¹ Setting aside that choice of law issue, however, both the common law approach and the Recognition Acts provide several criteria that can preclude a U.S. court from refusing to recognize a foreign judgment for lack of personal jurisdiction over the defendant.⁴² These criteria identify activities by a defendant that make an assertion of personal jurisdiction by the rendering court presumptively reasonable.⁴³

The common law approach and the Recognition Acts also provide several discretionary grounds for nonrecognition, meaning the U.S. court may—but is not required to—treat them as precluding recognition of a foreign judgment.⁴⁴ Of particular relevance here, a U.S. court may decline to recognize a foreign country judgment if the judgment is “repugnant to the public policy” of the United States or of the U.S. state in which recognition is sought.⁴⁵

E. Recognition of foreign administrative orders

The Recognition Acts apply by their own terms to “judgments,” and thus cannot be used to recognize foreign administrative acts that have not been the subject of a final, conclusive, and enforceable judgment between the defendant and the party seeking recognition. As a result, in the absence of a treaty, the only basis for recognizing a foreign administrative act that has not been reduced to a “judgment” in a U.S. court is the common law.⁴⁶

As the Restatement (Third) of Foreign Relations Law and the Restatement (Fourth) of Foreign Relations Law acknowledge, however, the common law is unclear as to whether foreign administrative acts can be recognized in a U.S. court.⁴⁷ The reporter's notes to the Restatement (Fourth) explain that “[a] handful of State-court decisions have indicated that a final, conclusive and enforceable administrative determination can be eligible for recognition if the administrative

⁴⁰ See RESTATEMENT (THIRD) § 482(1)(b); RESTATEMENT (FOURTH) § 483(b); 1962 RECOGNITION ACT § 4(a)(2); 2005 RECOGNITION ACT § 4(b)(2).

⁴¹ See Monestier, *supra* note 13, at 1739-44; Part B.6, *infra*.

⁴² See RESTATEMENT (THIRD) §§ 482(1)(b), 421(2); 1962 RECOGNITION ACT § 5; 2005 RECOGNITION ACT § 5.

⁴³ See *infra* Part IV.B.1.

⁴⁴ See RESTATEMENT (THIRD) § 482(2); RESTATEMENT (FOURTH) § 484; 1962 RECOGNITION ACT § 4(b); 2005 RECOGNITION ACT § 4(c).

⁴⁵ RESTATEMENT (THIRD) § 482(2)(d); RESTATEMENT (FOURTH) § 484(c); 1962 RECOGNITION ACT § 4(b)(3); 2005 RECOGNITION ACT § 4(c)(3).

⁴⁶ John C. Reitz, *Recognition of Foreign Administrative Acts*, 62 Am. J. Comp. L. 589, 602 (Supp. 2014).

⁴⁷ RESTATEMENT (THIRD) § 481 cmt. f (“The rule [in favor of recognizing foreign court judgments] is less clear with regard to decisions of administrative tribunals, industrial compensation boards, and similar bodies.”); RESTATEMENT (FOURTH) § 481 cmt. f (explaining that the rule's application to the decisions of administrative tribunals is “less clear”).

body employed proceedings generally consistent with due process, at least if the person opposing recognition had an opportunity to obtain judicial review.”⁴⁸

The Restatement (Third) of Foreign Relations Law, however, confirms that the rule against recognizing foreign penal judgments applies equally to foreign administrative orders that impose fines or penalties, explaining that “[a]ctions may be penal in character . . . even if they do not result from judicial process, for example when a government agency is authorized to impose fines or penalties for violation of its regulations.”⁴⁹

F. Procedural considerations and burdens of proof

Under both the common law and the 2005 Recognition Act, the procedure for seeking recognition of a foreign country judgment as an original matter is to initiate a civil action in a U.S. court seeking such recognition.⁵⁰ A party to an already-existing proceeding in a U.S. court can also seek recognition by raising the issue in that proceeding, for instance through a counterclaim or cross-claim, or as an affirmative defense.⁵¹

Once the issue is before the U.S. court, the party seeking recognition bears the initial burden of establishing that the foreign judgment meets the foundational requirements for recognition under the common law and the Recognition Acts; namely, the judgment is final, conclusive, and enforceable in the rendering jurisdiction, and is not a judgment for taxes, fines, or penalties.⁵²

Once a party seeking recognition makes that showing, the burden shifts to the party resisting recognition to establish that the foreign judgment is subject to one or more of the mandatory or discretionary grounds for nonrecognition, such as lack of personal jurisdiction in the rendering forum or that the judgment is repugnant to U.S. public policy.⁵³

II. Recognition and Enforcement of GDPR Orders and Judgments in U.S. Courts—Considerations for Private Plaintiffs

⁴⁸ RESTATEMENT (FOURTH) § 481 Reporter’s Note 6 (citing *Alberta Sec. Comm’n v. Ryckman*, 30 P.3d 121, 126-127 (Ariz. Ct. App. 2001) and *Regierungspräsident Land Nordrhein-Westfalen v. Rosenthal*, 17 A.D.2d 145, 232 N.Y.S.2d 963 (1st Dep’t 1962)); see also *Petition of Breau*, 132 N.H. 351, 360, 565 A.2d 1044, 1050 (1989) (recognizing determination of Canadian administrative body regarding teacher’s lack of good moral character by giving preclusive effect to body’s findings in New Hampshire credential revocation proceedings).

⁴⁹ RESTATEMENT (THIRD) § 483 cmt. b.

⁵⁰ RESTATEMENT (FOURTH) § 482; 2005 RECOGNITION ACT § 6(a).

⁵¹ RESTATEMENT (FOURTH) § 482; 2005 RECOGNITION ACT § 6(b).

⁵² See RESTATEMENT (FOURTH) § 485(1); 2005 RECOGNITION ACT § 3(c). While the 1962 Recognition Act does not contain any specific provisions on the burden of proof, courts deciding cases under that Act also typically place the initial burden of establishing that a judgment is within the Act’s scope on the party seeking recognition. See *Brand, supra* note 8 at 524 (citing *Bridgeway Corp. v. Citibank*, 45 F. Supp. 2d 276, 285 (S.D.N.Y. 1999); *S.C. Chimexim S.A. v. Velco Enters., Ltd.*, 36 F. Supp. 2d 206, 212 (S.D.N.Y. 1999)).

⁵³ See RESTATEMENT (FOURTH) § 485(3); 2005 RECOGNITION ACT § 4(d).

This Part of the Commentary discusses the considerations that might influence a private plaintiff seeking to obtain recognition and enforcement of a GDPR order or judgment entered in the EU through an action commenced in a U.S. court. We discuss both the legal considerations—whether and how a private plaintiff can make a prima facie case for recognition and enforcement of a given GDPR order under the general principles discussed in Part I—and the practical issues that such a Plaintiff might consider when deciding whether and how to pursue a recognition and enforcement action.

A. General considerations for private causes of action

If a U.S.-based data controller or data processor lacks a physical presence, assets, or other financial ties to the EU, an EU plaintiff who desires to enforce any judgment or order issued by an EU court or supervisory authority will need to file a civil action in U.S. court. That plaintiff will first need to clear the jurisdictional hurdles that confront all would-be litigants in our court system.

First, the plaintiff will need to identify and commence the action a forum in which the defendant is subject to personal jurisdiction.⁵⁴ While a detailed discussion of personal jurisdiction is beyond the scope of this Commentary, in general personal jurisdiction in both federal and state courts will be governed by the law on personal jurisdiction that is in force in the state where the court is located,⁵⁵ and by the Due Process Clause of the United States Constitution.⁵⁶

Second, the Plaintiff will need to establish that the court has subject-matter jurisdiction over the action. As with personal jurisdiction, a detailed discussion of subject matter jurisdiction is beyond the scope of this Commentary. But one important threshold requirement to establish subject matter jurisdiction is standing to sue.

In federal court, Article III of the United States Constitution requires a plaintiff that a plaintiff establish standing to sue by demonstrating that she “(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.”⁵⁷ It appears no federal court has squarely addressed the question whether a party seeking to enforce a foreign judgment has standing to do so. It appears nonetheless highly likely that a party seeking to do so would be able to establish standing under at least these circumstances: (1) the judgment awards money damages to the plaintiff; and (2) the defendant is the party against whom the foreign judgment was issued. Under these circumstances, the plaintiff can convincingly argue that she has suffered an injury in fact, insofar as she has taken a money judgment that has not been satisfied, and the defendant’s failure to satisfy that judgment would be

⁵⁴ See, e.g., Restatement (Fourth) § 482 Reporter’s Note 3 (“A court entertaining a separate action to obtain recognition of a foreign judgment must obtain jurisdiction over every person on whom its decision will have conclusive effect.”)

⁵⁵ See, e.g., Fed. R. Civ. P. 4(k)(1)(a).

⁵⁶ See, e.g., *Daimler AG v. Bauman*, 134 S. Ct. 746 (2014); *Goodyear Tires Operations, S.A. v. Brown*, 131 S. Ct. 2846 (2011) and

⁵⁷ *Spokeo Inc. v. Robbins*, __ U.S. __, 136 S.Ct. 1540, 1547 (2015).

“fairly traceable” to that defendant.⁵⁸ Finally, recognition and enforcement of the judgment by the federal court would redress the injury caused by the defendant’s failure to satisfy it.

Although not governed by Article III, a substantial majority of state courts apply analogous standing requirements.⁵⁹ To that end, many of these courts also require that a plaintiff show he or she has suffered an injury that is attributable to the defendant’s conduct.⁶⁰ As in federal court, a plaintiff’s possession of a judgment issued in her favor by an EU court against the defendant should in most cases be sufficient to satisfy these state court standing requirements

The standing analysis can be more complicated, however, in cases that involve judgments obtained by representative bodies on individual data subjects’ behalf. To that end, GDPR Article 80 now expressly provides for one or more data subjects to be represented in a private GDPR enforcement action in EU courts by “a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects’ rights and freedoms with regard to the protection of their personal data.”⁶¹

Such a body, organization, or association can either be requested by a data subject to lodge a complaint and obtain compensation under Article 82 on that individual’s behalf,⁶² or may act independently on the behalf of individual or multiple data subjects to submit matters to a supervisory authority under Article 77, or to a court under Articles 78 and 79, as provided by the law of their local Member State.⁶³

To the extent a body, organization, or association that has obtained a judgment on individuals’ behalf in the EU seeks to obtain recognition and enforcement of that judgment in a U.S. court, its claims could be analyzed under the doctrine of “representational standing.” To that end, the United States has long recognized that groups or organizations can maintain actions on behalf of their members in federal court when certain conditions are met. In *Hunt v. Washington State Apple Advertising Com’n*,⁶⁴ the United States Supreme Court held that “...an association has standing to bring suit on behalf of its members when: (a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization’s purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit.” When a foreign organization seeks to maintain representational standing, U.S. courts often make an additional inquiry into the law of the

⁵⁸ Cf. *ACLI Gov’t Sec., Inc. v. Rhoades*, 653 F. Supp. 1388, 1390 (S.D.N.Y. 1987), *aff’d sub nom. ACLI Gov. v. Rhoades*, 842 F.2d 1287 (2d Cir. 1988) (providing that owner of the judgment against defendant had standing in action to pursue collection)

⁵⁹ See generally Wyatt Sassman, *A Survey of Constitutional Standing in State Courts*, 8 Ky. J. Equine, Agric. & Nat. Resources L. 349 (2016)

⁶⁰ *Id.*

⁶¹ GDPR art. 80.1.

⁶² See *id.*

⁶³ *Id.* art. 80.2.

⁶⁴ 97 S.Ct. 2434, 2441, 432 U.S. 333, 343 (U.S.N.C., 1977)

organization's place of incorporation to determine whether the organization is permitted to pursue claims on behalf of its members.⁶⁵ Significantly, when it an organization satisfies all of these requirements, the organization itself does not have to suffer an injury maintain standing; it merely has to show that its members have suffered an injury.

Assuming an EU Court or Supervisory Authority would has already deemed an organization competent to represent the interests of individual members prior to entering a judgment in its favor under Article 80, that organization could convincingly argue that it meets the requirements for representational standing under *Hunt*.

B. Data subject compensation claims under GDPR Article 82

Under GDPR Article 82, individuals can receive compensation for damages suffered because of a controller or processor's GDPR violation.⁶⁶ This Part provides an overview of this aspect of GDPR, and evaluates the enforceability in U.S. courts of money judgments issued by EU courts in favor of data subjects, or not-for-profit bodies who bring suit on their behalf, under GDPR Article 82.

1. Overview and general considerations

Prior to GDPR's implementation, claims for damages by individuals for privacy breaches were limited to claims against data controllers and did not apply universally across all EU Member States. This right was not widely exercised. However, GDPR Article 82 expanded the rights of individuals to seek compensation directly from both data controllers and data processors for "any material or non-material damage as a result of an infringement"⁶⁷ of GDPR, thereby increasing the scope of compensatory claims and the parties that they can be brought against.

Under GDPR, individuals or non-profit entities are permitted to file a direct legal claim for compensation in the courts of the Member State where the controller or processor is established or in the courts where the data subject(s) maintain a "habitual residence."⁶⁸ Claims for compensation need not be preceded by a determination of fault by a supervisory authority, or any other administrative or non-judicial finding or remedy.⁶⁹

⁶⁵ Cf. *Authors Guild, Inc. v. HathiTrust*, 755 F.3d 87 (2d Cir. 2014) (associations authorized by foreign law to administer their foreign members' copyrights had standing to bring action); *Matter of Oil Spill by Amoco Cadiz Off Coast of France on March 16, 1978*, 954 F.2d 1279, 1319–20 (7th Cir. 1992)

⁶⁶ GDPR art. 82.1.

⁶⁷ U.S. readers should be mindful that "material and immaterial" may not mean the same thing to those in the U.S. that they do to those in the EU. Perhaps a better way for a U.S. reader to consider these terms is "tangible" and "intangible." An immaterial injury, like an intangible one, can be substantial.

⁶⁸ GDPR art. 79.2. If the controller or processor is a public authority of a Member State exercising its public powers, an action must be brought in that Member State. *Id.*

⁶⁹ However, the recommended first course of action of any data subject who believes his or her GDPR rights have been violated would be to report a claimed violation to their supervisory authority for investigation.

"Data subjects should receive full and effective compensation for the damage they have suffered."⁷⁰ Compensation may be recovered for both pecuniary and nonpecuniary losses that might include (but are not limited to) claims for distress, anxiety, or reputational damage.⁷¹ There are no caps or limits on the amount of damages recoverable under GDPR.⁷²

Individuals considering filing a claim for compensation under Article 82 should consider the monetary and logistical burden required to enforce any compensatory judgment obtained, particularly if collecting on that judgment would require recognition by a U.S. court. As such, when considering a direct individual claim against a U.S.-based controller or processor, due consideration should be given as to whether that organization has a formal establishment or financial presence within the EU upon which a judgment can be executed.

Yet, as noted above, the ability for individual data subjects to band together through the use of representative not-for-profit bodies pursuant to Article 80, may provide an economically viable vehicle to secure access to U.S. courts for execution of GDPR compensatory judgments awarded by an EU court.

As discussed below, an EU party that is able to present a U.S. court with a compensatory monetary judgment issued by an EU court of competent jurisdiction does have a reasonable probability of securing recognition and enforcement of that order in the United States.

2. Enforceability under U.S. law

Of the various types of orders and judgments that can be issued under GDPR, EU-based plaintiffs are most likely to be able to establish a prima face case in U.S. courts for recognition of money judgments obtained through EU court proceedings under GDPR Article 82.

First, assuming they are final and conclusive between the parties, these judgments should qualify as judgments that grant recovery of a sum of money and therefore fall comfortably within the scope of both Recognition Acts and the common law approach.⁷³ To that end, examples of U.S. courts recognizing and enforcing foreign judgments from EU Member States by applying analyses that would likely be applied to Article 82 recognition and enforcement actions abound.⁷⁴

⁷⁰ *Id.*; Recital 146 ("The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation.").

⁷¹ European Commission, Policies, information and services, *available at* https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/can-my-company-my-organisation-be-liable-damages_en.

⁷² However, certain Member States may have civil damages caps that would apply to Article 82 claims.

⁷³ See Part II.A-B, *supra*.

⁷⁴ See, e.g. *De Fontbrune v Wofsy*, 838 F3d 992, 1005 (9th Cir. 2016) (finding that a French judgment awarding damages under the French concept of *astreinte* could be recognized under Californian law because it could "be seen as fulfilling a function akin to statutory damages in American copyright law"); *Societe d'Amenagement et de Gestion de Labri Nautique v. Marine Travelift Inc.*, 324 F. Supp. 3d 1004, 1005 (E.D. Wis. 2018) (recognizing French products

Second, these judgments are also unlikely to violate the rule against enforcing “penal” judgments because their primary purpose is to compensate data subjects—rather than punish the U.S.-based defendant—and they do not serve to benefit public authorities.⁷⁵

C. Injunctions and non-monetary orders issued under GDPR Article 79

In addition to compensation claims that would require a U.S. defendant to pay damages to EU data subjects, an EU-based plaintiff might also seek and obtain an injunction, or an order for specific performance, against a U.S.-based defendant under GDPR Article 79. This Part of the Commentary discusses these types of orders and evaluates their enforceability in U.S. courts.

1. Overview and general considerations

GDPR Article 79 guarantees each EU data subject the non-exclusive right to “an effective judicial remedy where he or she considers that his or her [GDPR] rights under have been infringed as a result of the processing of his or her personal data in non-compliance with [GDPR].”⁷⁶

While GDPR Article 82 provides for compensatory damages to data subjects for non-compliance, monetary payments may not, by themselves, provide an effective judicial remedy. In such cases, an EU court can issue injunctive orders to prevent ongoing violations, or orders for specific relief or performance which require a data controller or data processor to either take or cease taking specific actions.

2. Enforceability under U.S. law

Would or could a U.S. court enforce injunctions or orders for specific performance issued under GDPR Article 79? There is currently little basis for U.S. judicial enforcement of these types of orders.

As noted in Part I.B., the Recognition Acts apply only to judgments that grant or deny recovery of a sum of money. Non-monetary orders issued by courts under GDPR Article 79, therefore, cannot be recognized or enforced under the Recognition Acts. And while the common law may allow for these types of orders to be *recognized*—i.e., given legal effect for purposes such as res judicata or collateral estoppel—there is very little precedent for invoking the authority of a

liability judgment); *ABC Arbitrage S.A. v. Caen*, No. CV 16-07014 SJO (EX), 2017 WL 7803784, at *3 (C.D. Cal. Feb. 28, 2017) (finding compensatory damages for fraud and breach of contractual monetary awards enforceable).

⁷⁵ See RESTATEMENT (THIRD) § 483 cmt. b; see also *De Fontbrune*, 838 F3d at 1005 (Ninth Circuit, 2016) (“[T]he purpose of the award was not to punish a harm against the public, but to vindicate [the judgment creditor’s] personal interest in having his copyright respected and to deter further future infringements by [the judgment debtor].”); *Plata v. Darbun Enterprises, Inc.* 2014 WL 341667, *5 (Cal. Ct. App. Jan. 31, 2014) (“[T]he issue whether a monetary award is a penalty within the meaning of the [Recognition Act] requires a court to focus on the legislative purpose of the law underlying the foreign judgment. A judgment is a penalty even if it awards monetary damages to a private individual if the judgment seeks to redress a public wrong and vindicate the public justice, as opposed to affording a private remedy to a person injured by the wrongful act.”).

⁷⁶ GDPR art. 79.1.

U.S. court to lend its power to *enforcing* them against a U.S. defendant.⁷⁷ Even under the relatively permissive view of the Restatement (Second) of Conflict of Laws,⁷⁸ enforcing injunctions dealing with the processing of personal data might arguably run afoul of its mandate that to be enforced, an injunction must “not impose an undue burden upon the American court.”⁷⁹

Thus, while a private plaintiff may be able to make out a *prima facie* case for recognition of a foreign judgment imposing an injunction on a U.S. defendant, or ordering specific performance, the circumstances under which a U.S. court could actually provide that relief are limited.

III. Recognition and Enforcement of GDPR Orders and Judgments in U.S. Courts—Considerations for EU Supervisory Authorities

This Part of the Commentary discusses the considerations that might influence a supervisory authority seeking to obtain recognition and enforcement in a U.S. court of a GDPR order or judgment entered by that supervisory authority in the EU pursuant to an exercise of its corrective powers.

As above, we discuss both the legal considerations—whether and how a supervisory authority can make a *prima facie* case for recognition and enforcement of a given GDPR order given the general principles discussed in Part I—and the practical issues the supervisory authority might consider when deciding whether and how to pursue a recognition and enforcement action.

A. Overview and general considerations

GDPR grants supervisory authorities broad authority to exercise “corrective powers” for violations of GDPR’s requirements. GDPR Article 58.2(c)-(j) enumerates those “corrective powers” as follows:

- (c) to order the controller or the processor to comply with the data subject’s requests to exercise his or her rights pursuant to this Regulation;
- (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
- (e) to order the controller to communicate a personal data breach to the data subject;

⁷⁷ See Part I.B., *supra*.

⁷⁸ See *id.*

⁷⁹ RESTATEMENT (SECOND) OF CONFLICT OF LAWS §102 cmt. g (AM. LAW INST. 1971).

- (f) to impose a temporary or definitive limitation including a ban on processing;
- (g) to order a rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to GDPR Article 17.2 and Article 19;
- (h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to GDPR Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
- (i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case; [and]
- (j) to order the suspension of data flows to a recipient in a third country or to an international organi[z]ation.⁸⁰

These corrective powers are discretionary in nature and consist both of affirmative (clauses c-e, i) and prohibitive actions (clauses f-h, j). The former require affirmative acts of compliance by controllers or processors, while the latter impose restrictions on their activities. These powers are not plenary, but rather expressly subject to “appropriate safeguards, including effective judicial remedy and due process.”⁸¹ Further, GDPR Article 78 provides “each natural or legal person” with “the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.”⁸²

U.S.-based data controllers and data processors that have an establishment in the EU—and are thus subject to GDPR Article 3.1—are expected to designate a lead supervisory authority in the Member State of their main establishment.⁸³ Meanwhile, U.S.-based data controllers who lack an establishment in EU—but are subject to GDPR under Article 3.2 as a result of their activities directed into the EU—are required to register an EU representative with a supervisory authority in a Member State of their choosing in which they are offering goods or services, or monitoring the behavior of resident data subjects.⁸⁴ GDPR assumes that the U.S.-based entity will subject to the jurisdictional exercise of the supervisory authority’s powers under Article 58 within the EU, including the enforcement of monetary, injunctive, or specific performance remedies either directly or through judicial order.

⁸⁰ GDPR art. 58.2.

⁸¹ *Id.* art. 58.3.

⁸² *Id.* art. 78.1.

⁸³ *See* GDPR Recital 124.

⁸⁴ *See* GDPR art. 27.

As an alternative to enforcing a judgment within the U.S., a supervisory authority has other means to stop GDPR violations within EU territory, for example by issuing a cease and desist letter to domain registrars and web hosting companies located within the EU to block the websites of the offending organizations within EU territory. Such action is not unprecedented in the EU. By way of example, the Spanish Government blocked certain websites during the unauthorized Catalan referendum.⁸⁵ Organizations with an EU web presence but without any physical presence within the EU, should thus not assume that a supervisory authority has no alternative methods to enforce its action within EU territory.

B. Non-monetary orders issued under Article 58: enforceability under U.S. law

Would or could a U.S. court enforce a non-monetary order issued by a supervisory authority through an exercise of the corrective powers enumerated in GDPR Article 58.2? There is currently little, if any, basis for U.S. judicial enforcement of these types of orders, for at least three reasons.

First, to the extent a supervisory authority's non-monetary order has not been reduced to a final judgment through proceedings in a court of competent jurisdiction in the EU, there is very little precedent for the recognition of that order in a U.S. court. As noted in Part I.B., the Recognition Acts are generally limited to recognizing "judgments" that are final, conclusive, and enforceable in the rendering jurisdiction. And as discussed in Part I.E., there is very little precedent under the common law for recognizing administrative orders that have not been reduced to judgments.

Second, and as also noted in Part I.B., the Recognition Acts apply only to judgments that grant or deny recovery of a sum of money. Non-monetary orders issued under GDPR Article 58.2 therefore cannot be recognized or enforced under the Recognition Acts. And while the common law may allow for these orders to be *recognized*—given legal effect for purposes such as res judicata or collateral estoppel—there is little authority for invoking the authority of a U.S. court to lend its power to *enforcing* them against a U.S. defendant, especially when the order has not been reduced to a judgment in an EU court.⁸⁶ Even under the relatively permissive view of the Restatement (Second) of Conflict of Laws regarding the enforcement of foreign injunctions, some of the corrective powers—including for example an order to "bring processing operations into compliance" with GDPR,⁸⁷ or imposing a "ban on processing"⁸⁸—would seem to require a level of involvement by the U.S. court that would run afoul of its mandate that to be enforced, an injunction must "not impose an undue burden upon the American court."⁸⁹

⁸⁵ "Spanish authorities try to shutter Catalan referendum websites" Politico, 22 September 2017, *available at* <https://www.politico.eu/article/spanish-authorities-try-to-shutter-catalan-referendum-websites/>.

⁸⁶ See Part I.B., *supra*.

⁸⁷ GDPR Art. 58.2(d).

⁸⁸ GDPR Art. 58.2(f).

⁸⁹ RESTATEMENT (SECOND) OF CONFLICT OF LAWS §102 cmt. g (AM. LAW INST. 1971).

Third, an order issued by a supervisory authority using its corrective powers could run afoul of the rule against the recognition of penal judgments outlined in Part I.C. Orders to “bring processing operations into compliance” with GDPR under Article 58.2(d), or that impose a ban on processing under Article 58.2(g), for instance, would arguably be “penal” insofar as they are “in favor of a foreign state . . . and primarily punitive rather than compensatory in character,” and would require a U.S. court to scrutinize and enforce foreign public law.⁹⁰

In sum, a plaintiff seeking to enforce a non-monetary order issued by a supervisory authority under GDPR Article 58.2 would face several challenges.

C. Administrative fines issued under Articles 58.2(i) and 83: enforceability under U.S. law

GDPR Article 58.2(i) gives supervisory authorities the authority to issue an administrative fine “in addition to, or instead of” the non-monetary orders listed in the preceding Part, depending on the circumstances of each individual case. GDPR Article 83.1 provides that these fines should be “effective, proportionate and dissuasive.”⁹¹ To that end, GDPR Article 83.2 lists the criteria to be considered in determining whether to impose a fine and the amount. These include, *inter alia*, “the nature, gravity, and duration of the infringement,”⁹² “any relevant previous infringements by the controller or processor,”⁹³ the controller or processor’s “degree of cooperation with the supervisory authority,”⁹⁴ and “any other aggravating or mitigating factor applicable to the circumstances of the case.”⁹⁵ Taken together, these provisions would seem to demonstrate that administrative fines issued under GDPR are intended to be punitive—rather than compensatory—in character.

Assuming so, administrative fines almost certainly qualify as “penalties” that are subject to nonrecognition under the Recognition Acts, both of which expressly exclude foreign fines and penal judgments from their provisions for recognition.⁹⁶ They are also subject to nonrecognition under the common law.⁹⁷ These conclusions likely apply whether or not an administrative fine is incorporated into a court judgment.

Importantly, and as noted in Part I.C. above, the 2005 Recognition Act’s savings clause might still allow for a foreign penal judgment to be recognized under the common law.⁹⁸ And

⁹⁰ RESTATEMENT (THIRD) § 483 cmt. b.

⁹¹ GDPR art. 83.1.

⁹² *Id.* art. 83.2(a).

⁹³ *Id.* art. 83.2(e).

⁹⁴ *Id.* art. 83.2(f).

⁹⁵ *Id.* art. 83.2(k).

⁹⁶ 1962 RECOGNITION ACT § 1(2) (defining “foreign judgment” that is subject to recognition as excluding “a judgment for taxes, a fine, or other penalty”); 2005 RECOGNITION ACT § 3(b) (providing that the act does not apply “to the extent that the judgment is . . . a fine or other penalty”).

⁹⁷ See RESTATEMENT (THIRD) § 483; RESTATEMENT (FOURTH) § 489.

⁹⁸ See 2005 RECOGNITION ACT § 11 (“This Act does not prevent the recognition under principles of comity or otherwise of a foreign-country judgment not within the scope of this act.”).

under the Restatement (Third) of Foreign Relations Law, the common law rule against recognition of foreign penal judgments is permissive, rather than mandatory, insofar as it provides that courts in the United States “are not required” to recognize or enforce penalties rendered by courts of other states.⁹⁹ Thus, it is conceivable that a U.S. court could recognize and enforce an administrative fine under GDPR that had been reduced to a judgment in an EU court, provided that the judgment was not subject to nonrecognition on another mandatory or discretionary basis.

But enforcement of such a judgment would seem unprecedented: although U.S. courts sometimes *recognize* foreign penal judgments in the context of criminal prosecutions and sentencing,¹⁰⁰ no U.S. court appears to have ever *enforced* a foreign judgment or order that called for the payment of a fine to a foreign government body in the absence of a treaty that required it.

IV. Recognition and Enforcement of GDPR Orders and Judgments in U.S. Courts—Considerations for U.S.-based Organizations

As noted in the Introduction, a U.S. business can be subject to GDPR in one of two ways under GDPR Article 3. Under Article 3.1, a U.S. business is subject to GDPR if it has an “establishment” in the EU. Under Article 3.2, a U.S. business not “established” in the EU is subject to GDPR if it offers goods or services “in” the EU, or monitors their behavior. A U.S. businesses may also be subject to the GDPR under Article 28 where it serves as a processor for businesses within the scope of Article 3.

This Part of the Commentary provides an overview of the GDPR’s application under Articles 3 and 28 the factors a U.S. business should take into account in assessing whether to resist an effort to enforce a GDPR order or judgment against it in U.S. courts, and what defenses it might have to that enforcement.

A. Overview and general considerations

1. Application of GDPR under Article 3.1

A U.S. business can be “established” in the EU for purposes of GDPR under Article 3.1 without having any branches or subsidiaries in the EU. Specifically, GDPR applies to U.S. businesses if there is a “controller” or “processor” established in the EU, whether or not the data processing takes place in the EU.¹⁰¹ A business is established in the EU when it conducts “the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.”¹⁰² Accordingly, a U.S. business with regular activity in the EU,

⁹⁹ RESTATEMENT (THIRD) § 483 cmt. a (“No rule of United States law or of international law would be violated if a court in the United States enforced a judgment of a foreign court for payment of taxes or comparable assessments that was otherwise consistent with the standards of §§ 481 and 482.”).

¹⁰⁰ *Id.* at Reporter’s Note 3.

¹⁰¹ GDPR art. 3.1.

¹⁰² GDPR Recital 22.

with an online presence in the EU, or with an agent or single employee within the EU, might be “established” in the EU.¹⁰³ If that business processes personal data in the context of the activities of such an establishment, even if that processing is outside the EU, GDPR applies under Article 3.1.

The business’ presence, however, must be sufficiently substantial to trigger GDPR application. The existence of an establishment under GDPR will not be construed so broadly as to include non-EU business with only “the remotest links”¹⁰⁴ to data processing, such as the accessibility of a company’s website.¹⁰⁵ For example, a wholly owned subsidiary of a U.S. company, located and operated in the EU, would likely be subject to GDPR. Similarly, a U.S. company with an online sales platform with an EU office would likely be subject to GDPR, even if the sales platform processed the data in the U.S. However if it isn’t conducting other monitoring or marketing activities, a U.S. company promoting a product with websites in multiple languages would likely not be subject to GDPR under Article 3.1, even if purchases are made over that website, if the company does not have an office or stable arrangement in the EU. That analysis may change, however, if the website advertises those languages using the flags of EU nations or sells its products in Euros, Pounds or other EU-recognized currency.

Accordingly, in evaluating Article 3.1, U.S. businesses should first determine whether they process personal data. Second, they should determine whether there are links “between the activity for which the data is being processed and the activities of any presence of the organization in the Union.”¹⁰⁶ And, finally, determine the strength and nature of those links in analyzing whether GDPR applies.

2. Application of GDPR under Article 3.2

For businesses not established in the EU pursuant to Article 3.1, Article 3.2 sets forth two circumstances under which GDPR can apply. First, GDPR applies to entities engaged in “the offering of goods or services, irrespective of whether payment of the data subject is required, to such data subjects in the Union.”¹⁰⁷ Second, GDPR applies to entities engaged in “the monitoring of their behavior as far as their behavior takes place within the Union.”¹⁰⁸

In evaluating whether GDPR Article 3.2 applies, U.S. businesses must assess whether the offering of goods or services is directed at a person in the EU. Recital 23 to GDPR is instructive

¹⁰³ “In order to determine whether an entity based outside the Union has an establishment in a Member State, both the degree of stability of the arrangements and the effective exercise of activities in that Member State must be considered in the light of the specific nature of the economic activities and the provision of services concerned. This is particularly true for undertakings offering services exclusively over the Internet.” EDPB Guidelines 3/2018 on the Territorial Scope of the GDPR (“EDPB Guidelines 3/2018”) at 5, citing *Weltimmo v NAIH* (C- 230/14).

¹⁰⁴ EDPB Guidelines 3/2018 at 6.

¹⁰⁵ *Id.* at 5, citing 0 CJEU, *Verein für Konsumenteninformation v. Amazon EU Sarl*, Case C 191/15, 28 July 2016, paragraph 76.

¹⁰⁶ *Id.* at 7.

¹⁰⁷ GDPR art. 3.2(a).

¹⁰⁸ *Id.* art. 3.2(b).

on how to undertake such an assessment, stating that “it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects” in the EU. It continues: “use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.” However, GDPR also cautions that “the mere accessibility of the controller’s, processor’s, or an intermediary’s website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention” to target EU individuals.¹⁰⁹ Therefore, it appears that the processor or controller must take affirmative steps to direct the goods and services at persons in the EU.¹¹⁰

EDPB Guidelines 3/2018 offers an example of such application. It suggests that if a U.S.-based company, without any presence or establishment in the EU, offers an app that processes EU users’ personal data in connection with a service, it falls within the scope of GDPR under Article 3.2. The EDPB, cautions, however, that the mere fact of processing personal data of an EU individual is not sufficient to trigger the application of GDPR. Instead, the U.S. business must have been “‘targeting’ individuals in the EU, either by offering goods or services to them or by monitoring their behavior.”¹¹¹

Article 3.2(b) states that GDPR also applies to non-EU business that “monitor [the] behavior” of data subjects as far as that behavior takes place within the EU.¹¹² Behavior monitoring includes tracking a person on the internet, and using their personal data to profile them “in order to take decisions concerning her or him for analyzing or predicting her or his personal preferences, behaviors and attitudes.”¹¹³ The EDPB Guidelines note that, in contrast to Article

¹⁰⁹ GDPR Recital 23.

¹¹⁰ EDPB Guidelines 3/2018 noted that the standards enumerated in Recital 23 is akin to those in existing Court of Justice of the European Union (“CJEU”) case law. Therefore, it refers to the following factors when assessing whether the goods or services are directed at a person in the EU: (1) the EU or at least one Member State is designated by name with reference to the good or service offered; (2) the data controller or processor pays a search engine operator for an internet referencing service in order to facilitate access to its site by consumers in the Union; or the controller or processor has launched marketing and advertisement campaigns directed at an EU country audience; (3) the international nature of the activity at issue, such as certain tourist activities; (4) The mention of dedicated addresses or phone numbers to be reached from an EU country; (5) the use of a top-level domain name other than that of the third country in which the controller or processor is established, for example “.de”, or the use of neutral top-level domain names such as “.eu”; (6) the description of travel instructions from one or more other EU Member States to the place where the service is provided; (7) the mention of an international clientele composed of customers domiciled in various EU Member States, in particular by presentation of accounts written by such customers; (8) the use of a language or a currency other than that generally used in the trader’s country, especially a language or currency of one or more EU Member States; and (9) the data controller offers the delivery of goods in EU Member States.

¹¹¹ EDPB Guidelines 3/2018 at 14.

¹¹² GDPR art. 3.2(b).

¹¹³ GDPR Recital 24.

3.2(a), there is no requirement that the data processor have intent to target behavior within the EU, yet also notes that “monitoring” implies that the data controller “has a specific purpose in mind.”¹¹⁴

3. Application of GDPR Under Article 28

Article 28 imposes GDPR obligations on processors performing processing for controllers that fall within the scope of Article 3, and it imposes obligations on subprocessors who perform processing on behalf of any processors falling within the scope of Article 3 or Article 28.¹¹⁵ Article 28 obligations are mandatory even if the processor or subprocessor is not independently captured within the scope of Article 3. Under Article 28.3, processing by any processor “shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller...”¹¹⁶ Both controllers engaging processors and processors engaging subprocessors must impose contractual obligations on their vendors “providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this Regulation.”¹¹⁷ Article 28 also hold processors fully accountable for any failures on the part of their subprocessors.¹¹⁸

Because of the broad scope of Article 28, a number of U.S. organizations that do not fall within the territorial scope of Article 3 may still find themselves required to execute agreements binding them to satisfy GDPR requirements with respect to certain types of processing activities. The enforcement of Article 28 agreements is discussed in more detail in Part V.B.2.

4. General Considerations

The right to privacy has long been an emotive subject for EU nationals. The right was first codified in Europe in Article 19 of the Universal Declaration of Human Rights in 1948. It was then included in Article 8 of the European Convention on Human Rights in 1950. Within the EU there was widespread support for the inclusion of the right to privacy in the European Convention on Human Rights, following the horrors of World War II and the selection of individuals for death based on their racial and medical background during the holocaust. GDPR stems from that history and the importance of the right to privacy for EU nationals given this context should not be underestimated.¹¹⁹

EU consumers have been known to boycott companies that consumers feel are avoiding their moral obligations via the use of legal loopholes. Take for example the boycott by British

¹¹⁴ EDPB Guidelines 3/2018 at 18.

¹¹⁵ GDPR art. 28.

¹¹⁶ *Id.*

¹¹⁷ *Id.*

¹¹⁸ *Id.*

¹¹⁹ “The GDPR Is Just the Latest Example of Europe’s Caution on Privacy Rights. That Outlook Has a Disturbing History”, *available at* <http://time.com/5290043/nazi-history-eu-data-privacy-gdpr/>.

consumers of Amazon¹²⁰ and Starbucks¹²¹ in 2013 and 2014, due to public concerns about the use of complex, but legal tax, structures to avoid or minimize the payment of a corporation tax on UK sales. A similar situation could foreseeably arise for U.S. organizations with a consumer base within the EU where they willfully and publicly refuse to recognize the enforceability of GDPR in actions taken by EU regulators or courts.

B. Key defenses to a recognition action

In addition to the practical and operational considerations above, a U.S.-based organization faced with an attempt by a private plaintiff or supervisory authority to obtain recognition in a U.S. court of an EU order or judgment entered under GDPR should consider the available legal defenses.

First, the U.S. organization should consider whether the plaintiff can establish a *prima facie* case for recognition, as the party seeking recognition of a foreign order or judgment bears that initial burden.¹²² The issues the plaintiff might face—and that a defendant might exploit—in that regard are discussed in Parts II.B.2., II.C.2., III.B., and III.C.

Assuming the plaintiff can establish a *prima facie* case for recognition, however, the burden switches to the U.S. defendant to establish that the judgment or order is subject to one of the mandatory or discretionary grounds for nonrecognition.¹²³ To that end, two grounds—one mandatory and one discretionary—seem especially likely to be available to U.S. defendants: (1) lack of personal jurisdiction over the defendant in the rendering forum, and (2) repugnancy of the EU order or judgment to U.S. public policy.

1. Lack of personal jurisdiction over the defendant in the EU

Under the common law and the Recognition Acts, lack of personal jurisdiction is a mandatory ground for nonrecognition of a foreign judgment.¹²⁴ Thus, a U.S. court will recognize a foreign judgment only if the foreign court had personal jurisdiction over the party against whom the judgment is to be enforced. A key issue in that regard is what law controls that question: the law of the country in which the judgment was rendered, or U.S. law.¹²⁵ The common law and the Recognition Acts diverge somewhat on this point.

The Restatement (Third) of Foreign Relations Law takes the view that under the common law, a US court should look to both the law of the rendering state and U.S. law. To that end,

¹²⁰ “Amazon UK boycott urged after retailer pays just £4.2m in tax,” *The Guardian*, May 9, 2014, *available at* <https://www.theguardian.com/business/2014/may/09/margaret-hodge-urges-boycott-amazon-uk-tax-starbucks>.

¹²¹ “Starbucks Suffers First Ever UK Sales Fall In 2013 After Tax Boycott,” *Huffington Post*, April 25, 2014, *available at* https://www.huffingtonpost.co.uk/2014/04/25/starbucks-sales-fall-tax-boycott_n_5211525.html.

¹²² See Part I.F., *supra*.

¹²³ *Id.*

¹²⁴ See Part I.D., *supra*.

¹²⁵ For a comprehensive discussion of this question see Monestier, *supra* note 13.

Section 482 of the Restatement declares that a court in the United States “may not” recognize a foreign judgment if “the court that rendered the judgment did not have jurisdiction over the defendant in accordance with the law of the rendering state *and* with the rule set forth in § 421.”¹²⁶ Section 421 of the Restatement (Third), in turn, lists several grounds that make an exercise of personal jurisdiction over a defendant presumptively reasonable:

- (2) In general, a state’s exercise of jurisdiction to adjudicate with respect to a person or thing is reasonable if, at the time jurisdiction is asserted:
 - (a) the person or thing is present in the territory of the state, other than transitorily;
 - (b) the person, if a natural person, is domiciled in the state;
 - (c) the person, if a natural person, is resident in the state;
 - (d) the person, if a natural person, is a national of the state;
 - (e) the person, if a corporation or comparable juridical person, is organized pursuant to the law of the state;
 - (f) a ship, aircraft or other vehicle to which the adjudication relates is registered under the laws of the state;
 - (g) the person, whether natural or juridical, has consented to the exercise of jurisdiction;
 - (h) the person, whether natural or juridical, regularly carries on business in the state;
 - (i) the person, whether natural or juridical, had carried on activity in the state, but only in respect of such activity;
 - (j) the person, whether natural or juridical, has carried on outside the state an activity having a substantial, direct, and foreseeable effect within the state, but only in respect of such activity; or
 - (k) the thing that is the subject of adjudication is owned, possessed, or used in the state, but only in respect of a claim reasonably connected with that thing.¹²⁷

¹²⁶ RESTATEMENT (THIRD) § 482(1)(b) (emphasis added).

¹²⁷ *Id.* § 421(2).

In addition, Section 421 of the Restatement provides that a defense of lack of jurisdiction is generally considered to be waived “by any appearance by or on behalf of a person . . . if the appearance is for a purpose that does not include a challenge to the exercise of jurisdiction.”¹²⁸

Thus, under the Restatement (Third)’s construction, a U.S. court first inquires whether the foreign court had personal jurisdiction under its own law, and then whether the exercise of that jurisdiction is “reasonable” in accordance with standards provided by U.S. common law and as set out in the Restatement.

The Restatement (Fourth), by contrast, suggest that only U.S. law governs the question of personal jurisdiction. Its rule makes no mention of the rendering state’s law regarding personal jurisdiction, and its comments provide that “[c]ourts in the United States will not recognize a foreign judgment if the court rendering the judgment would have lacked personal jurisdiction under the minimum requirements of due process imposed by the constitution.”¹²⁹

Both Recognition Acts also prohibit a U.S. court from recognizing a judgment rendered by a foreign court that lacked personal jurisdiction over the defendant.¹³⁰ Neither Recognition Act identifies the source of law that should govern that question in the U.S. court. Like the Restatement (Third), however, the Recognition Acts identify several factors that, once established, prohibit nonrecognition for lack of personal jurisdiction. Under the 2005 Recognition Act, for instance, a U.S. court “may not” refuse to recognize a foreign judgment for lack of personal jurisdiction if:

- (1) the defendant was served with process personally in the foreign country;
- (2) the defendant voluntarily appeared in the proceeding, other than for the purpose of protecting property seized or threatened with seizure in the proceeding or of contesting the jurisdiction of the court over the defendant;
- (3) the defendant, before the commencement of the proceeding, had agreed to submit to the jurisdiction of the foreign court with respect to the subject matter involved;
- (4) the defendant was domiciled in the foreign country when the proceeding was instituted or was a corporation or other form of business organization that had its principal place of business in, or was organized under the laws of, the foreign country; [or]
- (5) the defendant had a business office in the foreign country and the proceeding in the foreign court involved a [cause of action] [claim for relief]

¹²⁸ RESTATEMENT (THIRD) § 421(3).

¹²⁹ RESTATEMENT (FOURTH) § 483(b) and cmt. e.

¹³⁰ 1962 RECOGNITION ACT § 4(a)(2); 2005 RECOGNITION ACT § 4(b)(2).

arising out of business done by the defendant through that office in the foreign country[.]¹³¹

As to this choice of law question, at least one commentator has argued—with some force—that a U.S. court generally should not attempt to resolve the question of whether the foreign court actually had jurisdiction over the defendant under its own laws.¹³² Perhaps more importantly for purposes of this Commentary, that same commentator has also argued that, even when U.S. courts purport to look to foreign law, the end result is the same: they rarely end their analysis at the question of the application of foreign law, and their decisions most often turn on the application of U.S. law to the question of whether the foreign court’s assertion of personal jurisdiction was “reasonable,” “permitted,” or consistent with a “minimum contacts” analysis.¹³³

Without opining on the usefulness, or lack of it, of an inquiry into the foreign state’s law, this Commentary focuses on the question whether a U.S. court will consider an EU Member State’s assertion of personal jurisdiction under Article 3 of GDPR to be reasonable or permitted under U.S. legal standards. In other words, the Commentary assumes that the assertion of personal jurisdiction by the hypothetical EU court is consistent with GDPR and the law of personal jurisdiction within the relevant EU Member State.

GDPR Articles 3.1 and 3.2 provide the most likely starting point for an EU court or DPA’s exercise of personal jurisdiction over a U.S. defendant.

a. Personal jurisdiction under GDPR Article 3.1

In the case of GDPR Article 3.1, the question appears fairly straightforward insofar as that provision relies on the existence of an “establishment” in the EU:

This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.¹³⁴

An assertion of personal jurisdiction on this basis would likely be held to be reasonable under the both the common law and the Recognition Acts:

- If the conduct at issue was “in the context of an establishment of a controller or a processor in the Union,” the existence of an “establishment” in the EU would likely support a finding that the defendant was “present in the territory of the state” for purposes of Section 421 of the Restatement.

¹³¹ 2005 RECOGNITION ACT § 5.

¹³² Monestier, *supra* note 13, at 1743-63.

¹³³ *Id.* at 1759-60.

¹³⁴ GDPR art. 3.1.

- Similarly, the 2005 Recognition Act’s view that the exercise of jurisdiction is permitted where the defendant “had a business office in the foreign country and the proceeding in the foreign court involved a [cause of action] [claim for relief] arising out of business done by the defendant through that office in the foreign country” would appear to be satisfied whenever Article 3 paragraph 1 is triggered by the existence of an “establishment” in the EU.

Granted, GDPR Article 3 purports to apply “regardless of whether the processing takes place in the Union or not” while the Recognition Act requires that the cause of action arise out of business “done by the defendant through that office in the foreign country.” However, the Recognition Act’s use of the word “through,” rather than “in,” would likely apply to a showing that the processing was “in the context of the activities of an establishment” of the defendant. The fact that the processing itself did not take place “in” that establishment would seem to be of little help to a defendant if that processing was “in the context of the activities of” that establishment.¹³⁵

b. Personal jurisdiction under Article 3.2

GDPR Article 3.2, by contrast, provides a likely more controversial basis for an exercise of personal jurisdiction over a U.S.-based defendant, because neither of its grounds for application of GDPR requires the physical presence of that defendant within the EU. That provision provides:

This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- b. the monitoring of their behaviour as far as their behaviour takes place within the Union.¹³⁶

As an illustrative—and common—scenario in which the issue of the issue of personal jurisdiction could be especially relevant, consider a U.S.-based retailer operating a website accessible to data subjects within the EU but with no physical presence in the EU.

Under the Recognition Acts, the retailer could argue persuasively that none of the criteria for the permissible exercise of jurisdiction are present absent some showing of personal service within the EU or some appearance in the EU proceedings other than for the purpose of contesting jurisdiction.

¹³⁵ Precisely what it might mean for processing that does not take place “in” a particular business establishment to nonetheless be “in the context of the activities of” that establishment is a question of the substantive application of GDPR that is beyond the scope of this Commentary.

¹³⁶ GDPR art. 3.2.

The situation under the common law may, perhaps, be slightly more favorable for the party seeking to enforce the judgment or order, if that party could show that the defendant’s “offering of goods or services” to data subjects in the EU constituted “regularly carr[ying] on business” within the EU for purposes of Section 421(h) of the Restatement (Third) of Foreign Relations Law. Application of GDPR Article 3.2(a), however, is not restricted to situations in which the controller or processor “regularly” offers goods or services, and it is therefore likely that GDPR at least in some instances facially purports to extend its effect to U.S. businesses in a manner in which most U.S. courts would be unlikely to recognize.

A successful challenge to personal jurisdiction would seem even more likely with respect to an assertion of jurisdiction over a U.S. business under GDPR Article 3.2(b) based on the “monitoring of behavior” of data subjects within the EU, particularly if the business does not actively offer goods or services within the EU. Assume, for example, that a US business uses data supplied to it by a business in Canada, who in turn received the data from a source within the EU, to monitor the purchasing activities of French and German residents, and then provides reports to that Canadian company about that monitoring. GDPR Article 3.2(b) arguably applies to that U.S. business, but under either the Restatement’s or the Recognition Act’s approach it is quite doubtful that a US court would recognize a judgment taken against that U.S. business in a court within the EU. In the hypothetical, the US business would satisfy none of the criterion required for a “reasonable” assertion of personal jurisdiction under the Restatement (Third) of Foreign Relations Law or a “permitted” one under the Recognition Acts.

c. DPOs and Article 27 representatives: impact on personal jurisdiction in the EU

A U.S. entity that does not trigger any of the standards that make an assertion of jurisdiction presumptively reasonable through its day-to-day operations might nonetheless submit itself to jurisdiction of an EU court or regulator through the appointment of an agent in the EU. To that end, the comments and reporters’ notes to the Restatement (Third) of Foreign Relations Law suggest that conducting activity in a foreign state through an “agent” could be a basis to find a waiver of lack of personal jurisdiction as a ground for nonrecognition.¹³⁷

Two potential grounds for this “agency” theory of waiver are the defendant’s appointment of a “representative” in the EU pursuant to GDPR Article 27 or the designation of a Data Protection Officer (“DPO”) under GDPR Article 37.

Under GDPR Article 27, an EU representative appointed by a controller or processor not established in the EU, “shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.”¹³⁸ Arguably, at least, this could be seen as either the express or the implied

¹³⁷ See RESTATEMENT (THIRD) §§ 481, Reporter’s Note 3; 482, comment c.

¹³⁸ GDPR art. 27.4.

expression of consent to submit to personal jurisdiction within the Member State where the representative is appointed, particularly because the appointment is “without prejudice to legal actions which could be initiated against the controller or the processor themselves.”¹³⁹ The mandate that the representative is “to be addressed” by data subjects and supervisory authorities “for the purposes of ensuring compliance with this Regulation” is likely to be seen as a voluntary designation of an agent for the purpose of securing personal jurisdiction over the appointing entity.

Similarly, among the responsibilities of a DPO designated under GDPR Article 37 is that she “cooperate with the supervisory authority,” she “act as the contact point with the supervisory authority on issues relating to processing,” and she be available for contact by data subjects “with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.”¹⁴⁰ This, too, may be sufficient to imply consent to jurisdiction. Even if not, when a DPO is physically present in the EU, that presence may allow for personal service on the organization through an agent or at a place of business, a sufficient basis for personal jurisdiction under both the Restatement and the Recognition Acts.

US business are thus faced with somewhat of a catch-22. Appointment of an Article 27 representative and/or an Article 37 DPO may be required under GDPR and—even when not strictly required—could be seen as a prudent prophylactic against a GDPR-related complaints, lawsuits or enforcement actions. Simultaneously, however, it could supply a basis for the assertion of personal jurisdiction where no such basis otherwise existed. The very act of compliance with these provisions could potentially expose a U.S.-based business to the jurisdiction of a court within the EU when non-compliance could insulate it from judgments issued by EU courts.

2. Repugnancy to federal or state public policy

Under both the common law and the Recognition Acts, a U.S. court may decline to recognize a foreign country judgment if the judgment is “repugnant to the public policy” of the United States or of the U.S. state in which recognition is sought.¹⁴¹ “Repugnancy,” however, is a stringent standard.¹⁴² Courts have held that simple “inconsistency” between state or federal law and the foreign law does not render a foreign judgment unenforceable because of “repugnancy.”¹⁴³

¹³⁹ *Id.* art. 27.5.

¹⁴⁰ GDPR arts. 38.4; 39.1(d).

¹⁴¹ RESTATEMENT (THIRD) § 482(2)(d); RESTATEMENT (FOURTH) § 484(c); 1962 RECOGNITION ACT § 4(b)(3); 2005 RECOGNITION ACT § 4(c)(3).

¹⁴² RESTATEMENT (FOURTH) § 484 cmt. e (“The test for public policy is therefore a stringent one. . . . A foreign judgment violates local public policy only if its recognition would tend clearly to injure public health, public morals, or public confidence in the administration of law, or would undermine settled expectations concerning individual rights.”).

¹⁴³ See, e.g., *Naoko Ohno v. Yuko Yasuma*, 723 F.3d 984 (9th Cir. 2013) (“California courts have set a high bar for repugnancy under the Uniform Act. The standard . . . measures not simply whether the foreign judgment or cause of action is contrary to our public policy, but whether either is *so* offensive to our public policy as to be ‘prejudicial to recognized standards of morality and to the general interests of the citizens.’”); *Loucks ex rel. Loucks v. Standard Oil Co. of N.Y.*, 120 N.E. 198 (N.Y. 1918) (Cardozo, J.) (“We are not so provincial as to say that every solution of a problem is wrong because we deal with it otherwise at home.”).

But although repugnancy presents a high bar, there are several examples of cases in which courts have repugnancy as the basis for non-recognition of foreign judgments.¹⁴⁴

As one obvious potential area of “repugnancy,” enforcement of foreign judgments or administrative orders issued under GDPR may raise serious questions under the First Amendment. One example of such a question arises from the “right to be forgotten” under GDPR Article 58.2(g). Any such order would likely be repugnant to public policy because it might violate the First Amendment as a prior restraint.¹⁴⁵

Repugnancy to public policy may also be reflected in the Securing the Protection of Our Enduring and Established Constitutional Heritage (SPEECH Act), 22 U.S.C. §§ 4101-05. Interpreted broadly, the SPEECH Act suggests that all foreign judgments that would violate the First Amendment or chill free speech could be unenforceable through the US court system if those cases are deliberately brought in jurisdictions whose laws are less protective of free speech — as would likely be the case with right to be forgotten actions brought against US companies abroad.¹⁴⁶

GDPR orders and judgments could also raise due process concerns, depending on the procedures used in the EU to issue or obtain them.¹⁴⁷

V. Alternative Routes to GDPR Enforcement in U.S. Courts: The Federal Trade Commission, Privacy Shield, and Contract Claims

Where a U.S.-based organization has violated GDPR, there may be mechanisms for obtaining relief against that organization that do not, strictly speaking, arise under GDPR or involve the recognition or enforcement of GDPR judgments or orders. This Part of the Commentary discusses two significant possibilities in that regard: (1) enforcement by the U.S. Federal Trade Commission or individual data subjects of rights and obligations arising under the

¹⁴⁴ See, e.g., *Telnikoff v. Matusevitch*, 702 A.2d 230 (Md. 1997) (declining to enforce an English libel judgment under principles of comity because English defamation law is “totally different” from Maryland’s law “in virtually every significant respect” and “so contrary . . . to the policy of freedom of the press underlying Maryland law.”); *Pentz v. Kuppinger*, 31 Cal. App. 3d 590 (Ct. App. 1973) (concluding that a Mexican decree of divorce was repugnant to California law when it required husband to continue to pay alimony even after remarriage of wife).

¹⁴⁵ See Kurt Wimmer, *Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers?*, 68 SYR. L.R. 545, 574 (2018) (“When a foreign judgment is one that would violate the First Amendment, courts have found that it violates public policy and is thus unenforceable. . . . Because an order or fine under GDPR related to the right to be forgotten would almost certainly violate the First Amendment, a U.S. court would likely refuse to enforce such an order from an EU court.”). Note also the Securing the Protection of Our Enduring and Established Constitutional Heritage (SPEECH Act), 22 U.S.C. §§ 4101-05, which interpreted broadly suggests that all foreign judgments that would violate the First Amendment or chill free speech should be unenforceable through the US court system if those cases are deliberately brought in jurisdictions whose laws are less protective of free speech — as would likely be the case with right to be forgotten actions brought against US companies abroad. See *id.* at 574-75.

¹⁴⁶ See *id.* at 574-75.

¹⁴⁷ See, e.g., *Koster v. Automark Indus., Inc.*, 640 F.2d 77 (7th Cir. 1981) (Dutch statute governing service of process on defendants who reside in foreign countries provided insufficient assurances of actual notice to comport with American due process requirements, and thus Dutch default judgment could not be enforced in United States courts).

EU-US Privacy Shield program; and (2) contract-based actions arising out of agreements that U.S.-based organizations enter for GDPR-related purposes.

A. The Federal Trade Commission and Privacy Shield remedies

Because the Federal Trade Commission (FTC) is the principal Agency in the U.S. charged with protecting privacy and is therefore also primarily responsible for enforcing the EU-U.S. Privacy Shield program (which is administered by the U.S. Department of Commerce), some may reason that the FTC might assist in efforts to collect judgments or secure other relief for GDPR violations. Perhaps the best way to consider this idea is to look first at the FTC and its general enforcement authority, then to consider EU-U.S. Privacy Shield and the enforcement mechanisms it contains.

The FTC enforces several privacy-related U.S. laws (e.g., the Fair Credit Reporting Act, and the Children's Online Privacy Protection Act, to name just two); but its primary enforcement authority in privacy and data security cases is based on Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices. Although the Agency has brought hundreds of privacy and data security enforcement cases over the past 25 years, it can only enforce laws that are within its jurisdiction. It does not have any power either to enforce non-U.S. laws or to bring actions on behalf of individual private persons who may have suffered a privacy or data breach-related injury.

Nothing in the preceding paragraph is inconsistent with the FTC's enforcement of EU-U.S. Privacy Shield. Under that program, parties certify that they will abide by the numerous EU-U.S. Privacy Shield Principles and Supplemental Principles that were carefully negotiated between the U.S. Government and the EU. Thus, all EU-U.S. Privacy Shield companies must be subject to the regulatory powers of the FTC, or the U.S. Department of Transportation; publicly declare their commitment to comply with the Principles; publicly disclose their privacy policies in line with the Principles; and fully implement them.

When the FTC brings an enforcement action against an EU-U.S. Privacy Shield-certified company – as it did over 40 times against Safe Harbor certified companies – the Agency bases its claims on the company's violation of Section 5 of the FTC Act, usually because the company has misrepresented its practices and has thus failed to live up to its commitments. The EU-U.S. Privacy Shield program also includes a commitment by the FTC to establish a point of contact with EU supervisory authorities and to prioritize its investigations of potential violations that supervisory authorities refer to the Agency. Through that mechanism, EU Authorities have an additional means of enforcing GDPR compliance by EU-U.S. Privacy Shield-certified companies, even if they cannot enforce their own orders in U.S. court proceedings.

Data Subjects also have potential remedies under EU-U.S. Privacy Shield. Specifically, Annex 1 to EU-U.S. Privacy Shield provides that data subjects have a right to Binding Arbitration if they have first complained to the relevant company, given it an opportunity to correct its actions, resorted to the (free) independent recourse mechanisms set up in Principle 7, then complained to the relevant supervisory authority and given the U.S. Department of Commerce an opportunity to

resolve the matter. The arbitrators in each instance are selected by the parties from a list of at least 20 arbitrators developed by the U.S. Department of Commerce and the European Commission and the ensuing Arbitration may be conducted over the telephone. Although the Arbitration Panel lacks any authority to grant monetary remedies to data subjects, it has the authority to impose non-monetary relief such as granting access, correction, deletion, or return of the personal data in question. EU-U.S. Privacy Shield companies are required to advise data subjects of their rights to Binding Arbitration and the procedures they need to follow to invoke those rights. At least with respect to EU-U.S. Privacy Shield companies that violate GDPR, these mechanisms can provide individual data subjects with a viable alternative to seeking enforcement of a judgment by a U.S. court.

Although the EU-U.S. Privacy Shield program provides many benefits to data subjects and the EU, its future is uncertain. In the second annual review of the EU-U.S. Privacy Shield Agreement¹⁴⁸ the European Commission raised a number of concerns in regard to the program's functioning. However, the EU does not appear to be ready to revoke the EU-U.S. Privacy Shield framework but continues to place pressure on the U.S. Administration to address their concerns as to the operation and strength of the implementation of this framework by the U.S. Department of Commerce and the FTC.

B. Contract actions associated with data protection

1. Contracts between data subjects and data controllers

There are myriad contractual arrangements entered between EU data subjects and data controllers on a daily basis that expressly involve the collection and retention of personal data. Some may be related to long-term, essential relationships, such as contracts for employment, housing, or financial arrangements. Others may be highly transactional in nature, such as the use internet browser tracking mechanisms and one-off online transactions. And there are those that occupy a middle space: ongoing relationships of a non-essential nature. Many of these are represented by the omnipresent “I Agree” button that must be clicked to use some new software for a computer or mobile device, or to sign up for an online SaaS service. These agreements often contain a hyperlink to a “privacy policy” that has been “incorporated by reference” to the

¹⁴⁸ Among other things, the Commission called on the U.S. Administration to identify a nominee to fill a permanent role as the Privacy Shield Ombudsman for this framework by 28 February 2019. *See* REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the second annual review of the functioning of the EU-U.S. Privacy Shield {SWD(2018) 497 final}, available at https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf. On January 18, 2019, the White House announced its intention to appoint a person to the role. *See* <https://www.whitehouse.gov/presidential-actions/president-donald-j-trump-announces-intent-nominate-individual-key-administration-posts/>. The European Data Protection Board responded to this announcement on January 24, 2019 stating that they “cannot currently consider that the Ombudsperson is vested with sufficient powers to remedy non-compliance.” “European Data Protection Board - Sixth Plenary session: Privacy Shield, Brexit, clinical trials Q&A, DPIA lists, guidelines on certification, EDPB answer to Australian SA on data breach notification”, available at https://edpb.europa.eu/news/news/2019/european-data-protection-board-sixth-plenary-session-privacy-shield-brexit-clinical_en.

agreement, and sets out the non-negotiable terms for processing personal data that are difficult to understand by even the most experienced attorneys.

A EU data subject who has established a contractual relationship with a controller that includes data protection provisions may seek to uphold his or her rights and the controller's obligations in regards to data protection by submitting a complaint with the local supervisory authority, or by exercising the remedies provided under GDPR in a court of competent jurisdiction. A data controller may seek to defend its actions based on the consent provided by the data subject during the formation of the contract. However, the nature of the action will, in nearly all cases, stem from an alleged GDPR violation rather than a breach of contract. As such, an EU data subject is unlikely to need to appear in U.S. courts to enforce a judgment stemming from a contract action against a U.S.-based data controller.

2. Contracts between data controllers and data processors

For every contractual relationship between a data subject and a data controller, there are often numerous processing agreements between that data controller and its data processors both in the EU and around the world, including in the U.S. While a data subject has the direct relationship with the data controller, it is the duty of the data controller to ensure that the data processor complies with its processing agreement, or in case of data transferred out of the EU, its contractual obligations under the applicable data transfer mechanism.

From the prospective of the EU, data controllers are required to enter into data processing agreements and data transfer agreements as necessary to enforce the rights of data subjects, and ensure the obligations of both the data controller, the data processor (and any sub-processors) to the data subjects.¹⁴⁹ Data processing agreements and all standard contract clauses contain choice of jurisdiction, choice of venue, and choice of law provisions, requiring that the data processor, wherever located, to submit to the jurisdiction, venue, and law of the EU data controller.

From an EU perspective, it is certainly less costly and complex to bring a claim for breach of contract where the governing law of the contract is within the EU, compared to the U.S. Given the increased costs for an EU party bringing an action for breach of contract where the governing law of the contract is within the U.S., an EU party is unlikely to take this course of action unless they are of the view that substantial damages could be obtained based on a cost-benefit analysis.

In the event that a data processing agreement fails to specify a jurisdiction and venue, and an alleged breach occurs, an EU data controller will be required to litigate the matter in accordance with applicable international principles, and must anticipate significant additional costs for litigation and execution of any judgment in the U.S.

¹⁴⁹ See Part IV.A.3, *supra*.

3. Contracts related to employment or engagement of DPOs and EU representatives

GDPR provides for the designation of a DPO for data controllers and data processors under specific circumstances.¹⁵⁰ The DPO is not required to be a full time employee of the data controller or data processor; he or she may be an employee but with other duties, or may be an outside provider engaged under a service contract.¹⁵¹ The DPO is required to have a direct reporting line to the “highest management level of the controller or processor” and cannot be “dismissed or penalized by the data controller or data processor for performing his tasks.”¹⁵²

A U.S.-based data controller or data processor that is subject to GDPR under the territorial provisions of Article 3.2 is required to designate in writing a representative located in the EU.¹⁵³ This representative must be established in one of the Member States where goods and services are being offered, or whose behavior is being monitored.¹⁵⁴

A contract between a DPO or EU Representative and a U.S.-Based data controller or processor should contain provisions setting forth a choice of jurisdiction, venue and law to address any disputes that may result in litigation. From an EU perspective, the existence and essence of the relationship stems from the need for the operation and enforcement of GDPR. As such, the appropriate legal jurisdiction for such employment or engagement contacts should, in general, be in the EU. Similarly, under most circumstances, the venue should be either the main establishment of the controller or processor in the EU or the location of the DPO or Representative within the EU. Under all circumstances, the choice of law for any issues arising out of GDPR must be the EU.

In the event that a DPO and their controller or processor are based in the U.S., it would be unreasonable to presume that the venue for any GDPR-enforcement related dispute, such as allegations of wrongful termination in violation of Article 38.3, must be in the EU. However, it should be noted that a DPO may nonetheless seek redress through the applicable SA. That action may lead to subsequent follow-on litigation in both the EU and the U.S. by the supervisory authority related to enforcement of fines or orders of injunctive relief against the data controller or data processor.

¹⁵⁰ GDPR art. 37.1.

¹⁵¹ *Id.* art. 37.6.

¹⁵² *Id.* art. 38.3.

¹⁵³ *Id.* art. 27.1.

¹⁵⁴ *Id.* art. 27.3.