The Sedona Conference Journal

Volume 22 Forthcoming 2021

The Sedona Conference Commentary on the Enforceability in U.S. Courts of Orders and Judgments Entered under GDPR

The Sedona Conference

January 2021
Final Post-Public-Comment Version

Recommended Citation:

The Sedona Conference, *Commentary on the Enforceability in U.S. Courts of Orders and Judgments Entered under GDPR*, 22 SEDONA CONF. J. 277 (forthcoming 2021).

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

THE SEDONA CONFERENCE COMMENTARY ON THE ENFORCEABILITY IN U.S. COURTS OF ORDERS AND JUDGMENTS ENTERED UNDER GDPR

A Project of The Sedona Conference Working Group on Data Security and Privacy Liability (WG11)

Author:

The Sedona Conference

Editors-in-Chief:

Alex M. Pearce

Contributing Editors:

Joseph A. Dickinson
Starr Turner Drum
Marcel Duhamel
Ronald J. Hedges
Eric P. Mandel
Shoshana E. Rosenberg
Meredith L. Schultz
David Shonka

Steering Committee Liaison:

Bob Cattanach

Staff Editors:

David Lumia
Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 11. They do not necessarily

represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

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

This publication may be cited as follows:

> The Sedona Conference, *Commentary on the Enforceability in U.S. Courts of Orders and Judgments Entered under GDPR*, 22 SEDONA CONF. J. 277 (forthcoming 2021).

PREFACE

Welcome to the January 2021 final version of The Sedona Conference *Commentary on the Enforceability of Orders and Judgments Entered under GDPR* ("*Commentary*"), a project of The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG11 is to identify and comment on trends in data security and privacy law, in an effort to help organizations prepare for and respond to data breaches, and to assist attorneys and judicial officers in resolving questions of legal liability and damages.

The Sedona Conference acknowledges Editor-in-Chief Alex Pearce for his leadership and commitment to the project. We also thank contributing editors Joseph Dickinson, Starr Drum, Marcel Duhamel, Ron Hedges, Eric Mandel, Shoshana Rosenberg, Meredith Schultz, and David Shonka for their efforts. We also thank Bob Cattanach for his contributions as Steering Committee liaison to the project. We thank Claire Spencer for her contributions.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG11 who reviewed, commented on, and proposed edits to early drafts of the *Commentary* that were circulated for feedback from the Working Group membership. Other members provided feedback at WG11 annual and midyear meetings where drafts of the *Commentary* were the subject of the dialogue.

The publication was also subject to a period of public comment. On behalf of The Sedona Conference, I thank all of them for their contributions.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG11 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, patent litigation, patent remedies and damages, and trade secrets. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
January 2021

TABLE OF CONTENTS

INTRODUCTION

This *Commentary* evaluates the enforceability in a United States 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[2] and in the U.S. on the factors—both legal and practical—that speak to the enforcement of GDPR mandates through U.S. legal proceedings.

The question how and under what circumstances GDPR mandates can be enforced through U.S. legal proceedings arises as a result of the GDPR's broad territorial scope. To that end, GDPR constitutes a "significant evolution" of the territorial scope of EU data protection law compared to its predecessor and reflects an intention "to ensure comprehensive protection of the rights of data subjects in the EU and to establish . . . a level playing field for companies active on the EU markets, in a

---

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 Re-pealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents [hereinafter GDPR].

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 plus Iceland, Liechtenstein and Norway (note: Switzerland has not ratified the EEA Agreement, and GDPR has no direct application in that country). *See General Data Protection Regulation incorporated into the EEA Agreement*, EUROPEAN FREE TRADE ASSOCIATION, July 6, 2018, 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.

context of worldwide data flows."[3] Because of this evolution in territorial scope, organizations based outside the EU—including in the U.S.—that previously were not subject to EU data protection rules, or the consequences of violating them, can now be subject to both. But as a recent report from the Internet & Jurisdiction Policy Network explains, "a state's ability to enforce its laws is often more limited than the claims it makes regarding the reach of its laws."[4] Questions will thus inevitably arise about how supervisory authorities and data subjects can enforce the GDPR against these non-EU organizations.

In some cases, the answer will be straightforward. When an organization maintains a branch, subsidiary, or other assets in the EU, European supervisory authorities and data subjects can enforce GDPR mandates against the organization within the EU's borders.

The answer is less clear, however, if an organization violates the GDPR but does not maintain a physical presence or other assets in the EU. In that case, EU supervisory authorities and data subjects could issue an order or obtain a judgment against the organization. But unless the organization is willing to comply voluntarily with that order or judgment, the supervisory authority or data subject may require foreign assistance to enforce it.

---

3. European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1, at 4 (Nov. 12, 2019), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf [hereinafter Territorial Scope Guidelines].

4. DAN JERKER B. SVANTESSON, INTERNET & JURISDICTION POLICY NETWORK, INTERNET & JURISDICTION GLOBAL STATUS REPORT 2019 59 (2019), https://www.internetjurisdiction.net/uploads/pdfs/GSR2019/Internet-Jurisdiction-Global-Status-Report-2019_web.pdf.

When the violator is a U.S.-based organization, one potential source of assistance is the U.S. court system. There is an established body of U.S. law concerning the recognition and enforcement by U.S. courts of foreign judgments in other contexts.

This *Commentary* addresses the application of that body of law to GDPR orders and judgments. It explores 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.

Part I of the *Commentary* provides an overview of GDPR's extraterritorial scope under GDPR Article 3 and briefly examines how EU supervisory authorities have interpreted that provision since GDPR entered into force in May 2018.

Part II addresses the state of the law in the U.S. regarding the recognition and enforcement of foreign country orders and judgments. As we explain, some states have addressed the issue by adopting statutes, and others have relied on the common law. Each approach, however, relies on a set of common principles. Part II describes 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 III, IV, and V address how those general principles apply to claims by private plaintiffs (Part III) and claims by EU supervisory authorities (Part IV), and the potential defenses they create for U.S. defendants (Part V).

Finally, Part VI briefly addresses the ways that GDPR's requirements might be enforced other than through the direct enforcement of an existing EU order or judgment entered under

GDPR. These could include contract-based claims arising from GDPR-mandated data processing agreements, and claims brought against U.S. organizations by the U.S. Federal Trade Commission (FTC) using and individual data subjects under the EU-U.S. Privacy Shield and using its authority under Section 5 of the FTC Act.

I. AN OVERVIEW OF GDPR'S EXTRATERRITORIAL SCOPE

A. GDPR's Territorial Scope under Article 3

GDPR Article 3 defines GDPR's territorial scope according to two key criteria: the "establishment" criterion under Article 3.1 and the "targeting" criterion under Article 3.2.[5]

Under GDPR Article 3.1, GDPR applies to "the processing of personal data in the context of the activities of an establishment of a controller or a processor in the [EU], regardless of whether the processing takes place in the Union or not."[6] Although GDPR does not specifically define "establishment" for this purpose, its recitals explain that the term implies "the effective and real exercise of activities through stable arrangements" in the EU.[7] "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."[8]

GDPR Article 3.2 extends the law to a controller or processor with no establishment in the EU, when the controller or processor processes the personal data of data subjects in the EU in connection with (a) the offering of goods or services to data subjects in the EU (irrespective of whether payment is required),[9] or (b) the monitoring of those data subjects' behavior when they are in the EU.[10] Both conditions imply the purposeful "targeting" of data subjects located within the EU by an organization outside

5. Territorial Scope Guidelines, *supra* note 3, at 4.
6. GDPR, *supra* note 1, art. 3.1.
7. *Id.*, Recital 22.
8. *Id*.
9. *Id.*, art. 3.2(a).
10. *Id.*, art. 3.2(b).

the EU, and focus on processing activities related to that targeting.[11]

Since GDPR entered into force in May 2018, the European Data Protection Board (EDPB)—an independent European body composed of representatives of member state supervisory authorities established under GDPR Article 68[12]—has issued Guidelines that interpret Article 3.[13] Those Guidelines confirm an organization outside the EU can trigger GDPR's extraterritorial application without engaging in extensive or significant activities—physical or virtual—within the EU's borders.

With respect to the "establishment" criterion under GDPR Article 3.1, the EDPB Guidelines explain that the threshold "can actually be quite low" and can be satisfied if a non-EU entity has "one single employee or agent" in the EU, "if that employee or agent acts with a sufficient degree of stability."[14] Put another way, "[t]he fact that the non-EU entity responsible for the data processing does not have a branch or subsidiary in a[n EU] Member State does not preclude it from having an establishment there within the meaning of EU data protection law."[15]

The EDPB's interpretation of the limits of the "targeting" criterion is similarly expansive. The Guidelines explain that the application of GDPR Article 3.2(a) depends on the controller or processor's "intention to offer goods or services" to data subjects in the EU, which can be shown through factors such as "the mention of an international clientele composed of customers domiciled in various EU member states," and offering delivery

11. Territorial Scope Guidelines, *supra* note 3, at 14.

12. GDPR, *supra* note 1, art. 68.1

13. Territorial Scope Guidelines, *supra* note 3.

14. *Id*. at 6.

15. *Id.* at 6–7.

of goods to EU member states.[16] The Guidelines also explain that "monitoring" sufficient to trigger application of GDPR Article 3.2(b) can include activities commonly performed through commercial websites, including behavioral advertisements and "online tracking through the use of cookies."[17]

Of particular note, the Guidelines also explain that a non-EU processor who would not otherwise fall within GDPR's scope can become subject to GDPR under Article 3.2(b) when a non-EU controller for which the processor provides processing services engages in targeting activities.[18] The Guidelines acknowledge that the decision to target individuals in the EU "can only be made by an entity acting as a controller."[19] They conclude, however, that a non-EU processor can fall within GDPR's scope under Article 3.2(b) when its processing activities on the controller's behalf are "related to carrying out the [controller's] targeting," even when those processing activities are limited to providing data storage to the controller.[20]

When an organization falls within GDPR's territorial scope under GDPR Article 3.2, GDPR Article 27 requires the organization to appoint a representative in the EU, subject to certain narrow exceptions.[21] The representative must be mandated to receive—on behalf of the non-EU controller or processor—requests and inquiries from EU supervisory authorities and data subjects on all issues related to processing that falls within GDPR's scope. In practical terms, this often means that the

16. *Id.* at 17.
17. *Id.* at 20.
18. *Id.* at 21.
19. *Id.*
20. *Id.*
21. GDPR, *supra* note 1, arts. 27.1, 27.2.

representative will pass those requests and inquiries on to the controller or processor to formulate a response that the representative will then pass to the inquirer. To be clear, the representative is not merely a receiver of legal process. In fact, GDPR provides that the representative "should be subject to enforcement proceedings in the event of non-compliance by the controller or processor."[22] Guidelines in turn explain that supervisory authorities can launch enforcement proceedings "through the representative" against the controller or processor, including by "address[ing] corrective measures or administrative fines and penalties imposed on the controller or processor . . . to the representative."[23]

The Guidelines also conclude that the representative's direct liability under GDPR is "limited to its direct obligations referred to in articles [sic] 30 [record keeping] and article 58(1)a [responding to orders of a supervisory authority] of the GDPR."[24] As the EDPB explains, the representative cannot itself be held directly liable for the controller or processor's GDPR violations because "the GDPR does not establish a substitutive liability of the representative in place of the controller or processor it represents."[25]

B. Enforcement Activity Directed at Non-EU Organizations

To date, there have been two notable instances of GDPR enforcement activity directed toward non-EU controllers with no discernible physical presence or assets in the EU. They offer

22. *Id.*, Recital 80.

23. Territorial Scope Guidelines, *supra* note 3, at 28.

24. *Id.*

25. *Id.* at 27–28.

contrasting views on the limitations on the reach of EU supervisory authorities' enforcement power under those circumstances.

First, according to reporting by *The Register* in November 2018, a United Kingdom (UK) data subject made a complaint to the UK Information Commissioner's Office (ICO) regarding the cookie consent practices on the website of *The Washington Post*.[26] According to the complaint, the *Post*'s website impermissibly tied readers' consent to the use of cookies, tracking, and advertising to access to the website's content.[27] The ICO, according the *The Register*'s reporting, agreed that the practice violated Article 7 of GDPR (which requires that consent be "freely given") and issued a written warning that directed the newspaper to change its practices.[28] The ICO concluded, however, that it had no ability to compel *The Washington Post*'s compliance with that direction, explaining in a statement to *The Register* that "[w]e hope that the *Washington Post* will heed our advice, but if they choose not to, there is nothing more we can do in relation to this matter."[29]

Second, in July 2018, the ICO served an enforcement notice on a Canadian company called Aggregate IQ Data Services Ltd. ("AIQ"), which contracted with various UK political organizations to target political advertising messages to UK data subjects

26. Rebecca Hill, *Washington Post offers invalid cookie consent under EU Rules—ICO*, THE REGISTER (Nov. 19, 2018), https://www.theregister.co.uk/2018/11/19/ico_washington_post/.

27. *Id*.

28. *Id*.

29. *Id*.

on social media.[30] That enforcement notice claimed that AIQ was subject to GPDR under Article 3.2(b),[31] and that the company's data collection and advertising activities violated various provisions of GDPR, including GDPR Articles 5, 6, and 14.[32] The enforcement notice demanded that AIQ cease processing any personal data of UK or EU citizens for the purposes of data analytics, political campaigning, or any other advertising purposes.[33]

As a report issued earlier by the ICO explained, however, AIQ initially contended that the company was "not subject to the jurisdiction of the ICO."[34] As a result, the ICO notified the Canadian government that AIQ refused to participate in the ICO's investigation, and Canadian privacy authorities subsequently announced investigations into the company's practices.[35]

Ultimately, the ICO issued a new enforcement notice against AIQ in October 2018 that "varie[d] and replace[d]" the July 2018 notice.[36] Notably, that new notice said nothing about the ICO's

30. United Kingdom Information Commissioner's Office, Enforcement Notice to AggregateIQ Data Services Ltd, (July 6, 2018), https://ico.org.uk/media/2259362/r-letter-ico-to-aiq-060718.pdf.

31. *Id.* at ¶ 2.

32. *Id.* at ¶¶ 9–12.

33. *Id.* at ¶ 14; Annex 1.

34. United Kingdom Information Commissioner's Office, Investigation into the use of data analytics in political campaigns: investigation update (July 11, 2018), https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf, at 37.

35. *Id*.

36. United Kingdom Information Commissioner's Office, Enforcement Notice to AggregateIQ Data Services Ltd, (Oct. 24, 2018), https://ico.org.uk/

jurisdiction. The notice also imposed far narrower sanctions on AIQ: rather than a complete ban on the relevant processing, the company would simply have to erase the personal data of individuals in the UK that was maintained on the company's servers.[37]

The contrast between *The Washington Post* and AIQ cases suggest that EU supervisory authorities' willingness to pursue enforcement actions against non-EU organizations may depend on various factors. Those may include the seriousness of the alleged violation, the willingness of a local regulator to cooperate in enforcement efforts, and the defendant's willingness to engage with EU and local authorities.

media/action-weve-taken/enforcement-notices/2260123/aggregate-iq-en-20181024.pdf.

37. *Id.* at ¶ 14; Annex 1.

II. RECOGNITION AND ENFORCEMENT OF FOREIGN JUDGMENTS IN U.S. COURTS: OVERVIEW OF CURRENT LAW

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 summarize those principles that are most relevant to the enforceability of a judgment or order entered by a court or other enforcement authority.

A. Origins of the law of recognition and enforcement of foreign judgments

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 basis to "recognize" the judgment domestically.[38] The Full Faith and Credit Clause in Article IV of the Constitution provides that basis for judgments rendered in any other court—state or federal—in the United States.[39]

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,

38. 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).

39. *See* U.S. CONST. art. IV § 1.

and its historical roots can be traced back to the U.S. Supreme Court's 1895 decision in *Hilton v. Guyot*.[40]

In *Hilton*, the U.S. Supreme Court concluded that absent 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."[41] 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 nation should not allow it full effect, the merits of the case should

40. 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)) [hereinafter Brand, *FJC Guide*].

41. *Hilton*, 159 U.S. at 163–64.

> not, in an action brought in this country upon the judgment, be tried afresh.[42]

Using *Hilton* as a "conceptual backdrop," U.S. 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.[43]

Courts in a minority of U.S. states—sixteen—follow the first approach.[44] They generally rely on *Hilton*, the Restatement (Third) of Foreign Relations Law[45] (recently succeeded by the Restatement (Fourth) of Foreign Relations Law[46]), and the Restatement (Second) of Conflict of Laws.[47]

The other thirty-four U.S. states and the District of Columbia have adopted one of two model recognition acts:[48] (1) the 1962 Uniform Foreign Money Judgments Recognition Act (the "1962

---

42. *Id.* at 123.

43. 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).

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

45. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW (Am. Law Inst. 1987) [hereinafter RESTATEMENT (THIRD)].

46. RESTATEMENT (FOURTH) OF FOREIGN RELATIONS LAW (Am. Law Inst. 2018) [hereinafter RESTATEMENT (FOURTH)].

47. RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 98 (Am. Law Inst. 1971) [hereinafter RESTATEMENT (SECOND)].

48. Brand, *The Continuing Evolution*, *supra* note 44, at 295.

Recognition Act"),[49] or (2) the 2005 Uniform Foreign-Country Money Judgments Recognition Act (the "2005 Recognition Act")[50] (collectively, the "Recognition Acts").

While U.S. law regarding foreign judgment recognition may thus seem to be a disparate patchwork,[51] 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 nonrecognition.

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.[52] A judgment is "final" for this purpose when it "is not subject to additional proceedings in the rendering court other than execution."[53] Both contested and default judgments can meet these criteria.[54] While being subject to an appeal "does not deprive it

---

49. Uniform Foreign Money-Judgments Recognition Act (Unif. Law Comm'n 1962) [hereinafter 1962 Recognition Act].

50. Uniform Foreign-Country Money Judgments Recognition Act (Unif. Law Comm'n 2005) [hereinafter 2005 Recognition Act].

51. Monestier, *supra* note 43, at 1735.

52. 1962 Recognition Act, *supra* note 49, § 2; 2005 Recognition Act, *supra* note 50, § 3(a)(2); RESTATEMENT (THIRD), *supra* note 45, § 481; RESTATEMENT (FOURTH), *supra* note 46, § 481.

53. RESTATEMENT (THIRD), *supra* note 45, § 481 cmt. e. *See also* RESTATEMENT (FOURTH), *supra* note 46, § 481 cmt. d.

54. *See* Brand, *FJC Guide*, *supra* note 40, 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

of its character as a final judgment,"[55] a U.S. court may—but need not—stay the recognition of a foreign judgment until the appeal has run its course in the rendering country.[56]

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.[57] 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.[58]

Whether and under what circumstances a U.S. court will *enforce* these nonmonetary 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

---

proper notice in the originating court, or other grounds for non-recognition otherwise available under the applicable statute or common law").

55. RESTATEMENT (THIRD), *supra* note 45, § 481 cmt. e.

56. 1962 Recognition Act, *supra* note 49, § 6; 2005 Recognition Act, *supra* note 50, § 8; RESTATEMENT (THIRD), *supra* note 45, § 481 cmt. e.; RESTATEMENT (FOURTH), *supra* note 46, § 481 cmt. e.

57. 1962 Recognition Act, *supra* note 49, §§ 1(2), 3; 2005 Recognition Act, *supra* note 50, § 3(a)(1).

58. RESTATEMENT (THIRD), *supra* note 45, § 481 cmt. b ("Judgments granting injunctions, declaring rights or determining status . . . may be entitled to recognition under this and the following sections."); RESTATEMENT (FOURTH), *supra* note 46, § 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), *supra* note 47, § 102 cmt. g ("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.").

relief ordered by the rendering court.[59] The Restatement (Second) of Conflict of Laws, by contrast, concludes that foreign injunctive decrees *can* be enforced as long as 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."[60] 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.[61]

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

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.[62]

A judgment is "penal" under this rule when it is "in favor of a foreign state or one of its subdivisions, and primarily punitive

---

59. RESTATEMENT (THIRD), *supra* note 45, § 481 cmt. b ("Judgments granting injunctions, declaring rights or determining status . . . are not generally entitled to enforcement."); RESTATEMENT (FOURTH), *supra* note 46, § 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.").

60. RESTATEMENT (SECOND), *supra* note 47, § 102 cmt. g.

61. *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).

62. *See* RESTATEMENT (THIRD), *supra* note 45, § 483; RESTATEMENT (FOURTH), *supra* note 46, § 489; 1962 Recognition Act, *supra* note 49, § 1(2); 2005 Recognition Act, *supra* note 50, § 3(b).

rather than compensatory in character."[63] 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."[64]

The Recognition Acts both expressly exclude foreign fines and penal judgments from their provisions for recognition.[65] The 2005 Recognition Act, however, includes a savings clause that leaves room to recognize these judgments on other grounds, such as comity under the common-law approach.[66]

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.[67] 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

63. RESTATEMENT (THIRD), *supra* note 45, § 483 cmt. b. *See also* RESTATEMENT (FOURTH), *supra* note 46, § 489 cmt. b.

64. RESTATEMENT (THIRD), *supra* note 45, § 483 reporter's note 2.

65. 1962 Recognition Act, *supra* note 49, § 1(2) (defining "foreign judgment" that is subject to recognition as excluding "a judgment for taxes, a fine, or other penalty"); 2005 Recognition Act, *supra* note 50, § 3(b) (providing that the act does not apply "to the extent that the judgment is . . . a fine or other penalty").

66. *Id*. § 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.").

67. RESTATEMENT (THIRD), *supra* note 45, § 483 ("Courts in the United States are not required to enforce [penal judgments].").

comparable assessments that was otherwise consistent" with the standards for recognition.[68]

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."[69]

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.

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.[70] 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.[71] 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.[72] These criteria identify activities by a defendant that make an assertion of

---

68. *Id.* § 483 cmt. a.

69. RESTATEMENT (FOURTH), *supra* note 46, § 489.

70. *See* RESTATEMENT (THIRD), *supra* note 45, § 482(1)(b); RESTATEMENT (FOURTH), *supra* note 46, § 483(b); 1962 Recognition Act, *supra* note 49, § 4(a)(2); 2005 Recognition Act, *supra* note 50, § 4(b)(2).

71. *See* Monestier, *supra* note 43, at 1739–44.

72. See RESTATEMENT (THIRD), *supra* note 45, §§ 482(1)(b), 421(2); 1962 Recognition Act, *supra* note 49, § 5; 2005 Recognition Act, *supra* note 50, § 5.

personal jurisdiction by the rendering court presumptively reasonable.[73]

The common-law approach and the Recognition Acts also provide several discretionary grounds for nonrecognition, meaning the U.S. court may—but need not—treat them as precluding recognition of a foreign judgment.[74] 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.[75]

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.[76]

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

---

73. *See* Part V.A, *infra*.

74. *See* RESTATEMENT (THIRD), *supra* note 45, § 482(2); RESTATEMENT (FOURTH), *supra* note 46, § 484; 1962 Recognition Act, *supra* note 49, § 4(b); 2005 Recognition Act, *supra* note 50, § 4(c).

75. RESTATEMENT (THIRD), *supra* note 45, § 482(2)(d); RESTATEMENT (FOURTH), *supra* note 46, § 484(c); 1962 Recognition Act, *supra* note 49, § 4(b)(3); 2005 Recognition Act, *supra* note 50, § 4(c)(3).

76. John C. Reitz, *Recognition of Foreign Administrative Acts*, 62 AM. J. COMP. L. 589, 602 (Supp. 2014).

administrative acts can be recognized in a U.S. court.[77] 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 body employed proceedings generally consistent with due process, at least if the person opposing recognition had an opportunity to obtain judicial review."[78]

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."[79]

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

---

77. RESTATEMENT (THIRD), *supra* note 45, § 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), *supra* note 46, § 481 cmt. f (explaining that the rule's application to the decisions of administrative tribunals is "less clear").

78. *Id*. § 481 Reporter's Note 6 (citing Alberta Sec. Comm'n v. Ryckman, 30 P.3d 121, 126–127 (Ariz. Ct. App. 2001) and Regierungspraesident Land Nordrhein-Westfalen v. Rosenthal, 232 N.Y.S.2d 963 (N.Y. 1st Dep't 1962)); *see also* Petition of Breau, 565 A.2d 1044, 1050 (N.H. 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).

79. RESTATEMENT (THIRD), *supra* note 45, § 483 cmt. b.

judgment is to initiate a civil action in a U.S. court.[80] 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.[81]

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: the judgment is final, conclusive, and enforceable in the rendering jurisdiction, and is not a judgment for taxes, fines, or penalties.[82]

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.[83]

---

80. RESTATEMENT (FOURTH), *supra* note 46, § 482; 2005 Recognition Act, *supra* note 50, § 6(a).

81. RESTATEMENT (FOURTH), *supra* note 46, § 482; 2005 Recognition Act, *supra* note 50, § 6(b).

82. *See* RESTATEMENT (FOURTH), *supra* note 46, § 485(1); 2005 Recognition Act, *supra* note 50, § 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, *FJC Guide, supra* note 40, 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)).

83. *See* RESTATEMENT (FOURTH), *supra* note 46, § 485(3); 2005 Recognition Act, *supra* note 50, § 4(d).

III. RECOGNITION AND ENFORCEMENT OF GDPR ORDERS AND JUDGMENTS IN U.S. COURTS: PRIVATE ACTIONS BY DATA SUBJECTS AND REPRESENTATIVE ORGANIZATIONS

This part of the *Commentary* explores the different kinds of GDPR orders and judgments that a private plaintiff—whether an individual EU data subject or a representative organization acting on behalf of a group of EU data subjects—might seek to enforce through a U.S. court and how U.S. law would apply to those orders and judgments.

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 and is unwilling to comply voluntarily with a judgment or order issued by an EU court or supervisory authority, an aggrieved EU plaintiff could file a civil action in a U.S. court seeking recognition and enforcement of that judgment or order within the United States. To succeed, that plaintiff will first need to clear the jurisdictional hurdles that confront all would-be litigants in the U.S. court system. First, the plaintiff will need to identify and commence the action in a forum in which the defendant is subject to personal jurisdiction.[84] 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

84. *See, e.g.*, RESTATEMENT (FOURTH), *supra* note 46, § 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.").

state where the court is located,[85] and by the Due Process Clause of the U.S. Constitution.[86]

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 U.S. Constitution requires 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."[87] 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 is nonetheless highly likely that a party seeking to do so would be able to establish standing when: (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 was awarded a money judgment that has not been satisfied, and the defendant's failure to satisfy that judgment would be "fairly traceable" to that defendant.[88] Finally, the party seeking

85. *See, e.g.*, FED. R. CIV. P. 4(k)(1)(a).

86. *See, e.g.*, Daimler AG v. Bauman, 571 U.S. 117 (2014); Goodyear Dunlop Tires Operations, S.A. v. Brown, 564 U.S. 915 (2011).

87. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).

88. *Cf.* ACLI Gov't Secs., 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).

damages could likely also show that 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 U.S. state courts apply analogous standing requirements.[89] To that end, many of these courts also require that a plaintiff show she has suffered an injury that is attributable to the defendant's conduct.[90] As in federal court, a plaintiff's possession of a judgment issued in her favor by an EU court against the defendant should 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. GDPR Article 80 expressly allows 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."[91] The organization must have been "properly constituted in accordance with the law of a Member State, ha[ve] statutory objectives which are in the public interest, and [be] active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data."[92]

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,[93] or may

89. *See generally* Wyatt Sassman, *A Survey of Constitutional Standing in State Courts*, 8 KY. J. EQUINE, AGRIC. & NAT. RESOURCES L. 349 (2016).

90. *Id.*

91. GDPR, *supra* note 1, art. 80.1.

92. *Id.*

93. *See id*.

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.[94]

If an organization that has obtained a judgment on behalf of data subjects 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 Commission*,[95] the U.S. 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 organization's place of incorporation to determine whether the organization is permitted to pursue claims on behalf of its members.[96] Significantly, when an organization satisfies all of these requirements, the organization itself does not have to suffer an injury to maintain standing; it merely has to show that its members have suffered an injury.

---

94. *Id.*, art. 80.2.

95. 432 U.S. 333, 343 (1977).

96. *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).

Given that the GDPR requires that the representative organization be "in the public interest" and "active in the field of the protection of data subjects' rights," and assuming an EU Court or Supervisory Authority has already found an organization to satisfy those requirements, 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 as a result of a controller's or processor's GDPR violation.[97] 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 EU data subjects 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. 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"[98] of GDPR, thereby increasing the scope of compensatory claims and the parties against whom they can be brought.

---

97. GDPR, *supra* note 1, art. 82.1.

98. 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"

Under GDPR, individuals or not-for-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."[99] Claims for compensation need not be preceded by a determination of fault by a supervisory authority, or any other administrative or nonjudicial finding or remedy.

GDPR provides that "[d]ata subjects should receive full and effective compensation for the damage they have suffered."[100] Compensation may be recovered for both pecuniary and non-pecuniary losses that might include, but are not limited to, claims for distress, anxiety, or reputational damage.[101] GDPR does not impose any caps or limits on the amount of damages recoverable by a data subject harmed by a controller's or processor's violation.

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.

---

and "intangible." An immaterial injury, like an intangible one, can be substantial.

99. GDPR, *supra* note 1, 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.*

100. *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.").

101. European Commission, Can my company/my organisation be liable for damages?, *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 (last visited Dec. 15, 2020).

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 facie 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.[102] Examples abound 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.[103]

Second, these judgments are 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.[104]

---

102. *See* Parts II.A & I.B, *supra*.

103. *See, e.g.*, de Fontbrune v. Wofsy, 838 F.3d 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 dAmenagement et de Gestion de lAbri Nautique v. Marine Travelift Inc., 324 F. Supp. 3d 1004, 1005 (E.D. Wis. 2018) (recognizing French products 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).

104. *See* RESTATEMENT (THIRD), *supra* note 45, § 483 cmt. b; *see also de Fontbrune*, 838 F.3d at 1005 ("[T]he purpose of the award was not to punish a harm against the public, but to vindicate [the judgment creditor's] personal

C. *Injunctions and nonmonetary 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 nonexclusive 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]."[105]

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

---

interest in having his copyright respected and to deter further future infringements by [the judgment debtor]."); Plata v. Darbun Enters., Inc., Case No. D062517, 2014 WL 341667, at *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.").

105. GDPR, *supra* note 1, art. 79.1.

2. Enforceability under U.S. law

As noted in Part II.B, the Recognition Acts apply only to judgments that grant or deny recovery of a sum of money. Even under the relatively permissive view of the Restatement (Second) of Conflict of Laws, 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."[106]

Thus, while a private plaintiff may be able to make 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.

106. RESTATEMENT (SECOND), *supra* note 47, § 102 cmt. g.

IV. RECOGNITION AND ENFORCEMENT OF GDPR ORDERS AND JUDGMENTS IN U.S. COURTS: CORRECTIVE ORDERS ENTERED BY EU SUPERVISORY AUTHORITIES

This part of the *Commentary* discusses the types of corrective orders that an EU supervisory authority might seek to enforce against a U.S. defendant through U.S. courts, and how U.S. law would apply to those orders.

A. Overview and general considerations

GDPR grants supervisory authorities broad authority to exercise "corrective powers" for violations of GDPR's requirements. Specifically, GDPR Article 58.2(c)-(j) enumerates "corrective powers":

> (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;
>
> (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 Article 17.2 and Article 19;

> (h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to 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 organisation.[107]

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 are expressly subject to "appropriate safeguards, including effective judicial remedy and due process."[108] 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."[109]

---

107. GDPR, *supra* note 1, art. 58.2.

108. *Id.*, art. 58.3.

109. *Id.*, art. 78.1.

B. Nonmonetary orders issued under Article 58: enforceability under U.S. law

Would or could a U.S. court enforce a supervisory authority's nonmonetary order under 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 nonmonetary 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 II.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 II.E, there is very little precedent under the common law for recognizing administrative orders that have not been reduced to judgments.

Second, as also noted in Part II.B, the Recognition Acts apply only to judgments that grant or deny recovery of a sum of money. Nonmonetary 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.[110] 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

110. *See* Part II.B, *supra.*

GDPR,[111] or imposing a "ban on processing"[112]— would seem to require a level of involvement by a 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."[113]

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 II.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.[114]

In sum, a plaintiff seeking to enforce a nonmonetary 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 nonmonetary orders listed in the preceding Section, depending on the circumstances of each individual case. GDPR Article 83.1 provides that these fines should be "effective, proportionate and dissuasive."[115] To that end, GDPR Article 83.2 lists the criteria to be considered in determining whether to

111. GDPR, *supra* note 1, art. 58.2(d).

112. *Id.*, art. 58.2(f).

113. RESTATEMENT (SECOND), *supra* note 47, § 102 cmt. g.

114. RESTATEMENT (THIRD), *supra* note 45, § 483 cmt. b.

115. GDPR, *supra* note 1, art. 83.1.

impose a fine and the amount. These include, *inter alia*, "the nature, gravity, and duration of the infringement,"[116] "any relevant previous infringements by the controller or processor,"[117] the controller or processor's "degree of cooperation with the supervisory authority,"[118] and "any other aggravating or mitigating factor applicable to the circumstances of the case."[119] Taken together, these provisions confirm that administrative fines issued under GDPR are punitive—rather than compensatory—in character.

Accordingly, administrative fines are in most circumstances subject to nonrecognition under the Recognition Acts, both of which expressly exclude foreign fines and penal judgments from their provisions for recognition.[120] They can also be subject to nonrecognition under the common law.[121] These conclusions likely apply whether or not an administrative fine is incorporated into a court judgment.

There is, however, a potential exception to the rule against recognizing foreign fines and penal judgments. As noted in Part II.C above, the 2005 Recognition Act's savings clause might still allow for a foreign penal judgment to be recognized under the

116. *Id.*, art. 83.2(a).

117. *Id.*, art. 83.2(e).

118. *Id.*, art. 83.2(f).

119. *Id.*, art. 83.2(k).

120. 1962 Recognition Act, *supra* note 49, § 1(2) (defining "foreign judgment" that is subject to recognition as excluding "a judgment for taxes, a fine, or other penalty); 2005 Recognition Act, *supra* note 50, § 3(b) (providing that the act does not apply "to the extent that the judgment is . . . a fine or other penalty").

121. *See* RESTATEMENT (THIRD), *supra* note 45, § 483; RESTATEMENT (FOURTH), *supra* note 46, § 489.

common law.[122] And 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.[123] 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,[124] 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.

---

122. *See* 2005 Recognition Act, *supra* note 50, § 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.").

123. RESTATEMENT (THIRD), *supra* note 45, § 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.").

124. *Id.* at Reporter's Note 3.

V. POTENTIAL DEFENSES UNDER U.S. LAW TO AN ACTION SEEKING RECOGNITION AND ENFORCEMENT OF A GDPR ORDER OR JUDGMENT

The party seeking to enforce the order or judgment bears the initial burden of establishing a prima facie case for recognition.[125] The issues the plaintiff might face—and that a defendant might exploit—in that regard are discussed in Parts II and III.

Assuming the plaintiff establishes a prima facie case for recognition, 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.[126] U.S. defendants might be especially likely to raise two grounds for nonrecognition, one mandatory and one discretionary: (1) that the rendering forum in the EU lacked personal jurisdiction over the defendant, and (2) that the order sought to be enforced is repugnant to U.S. public policy.

This part of the *Commentary* provides an overview of those defenses.

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

Under the common law and the Recognition Acts, lack of personal jurisdiction over the defendant in the rendering court is a mandatory ground for nonrecognition of a foreign judgment in a U.S. court.[127] 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.

---

125. *See* Part II.F, *supra*.

126. *Id*.

127. *See* Part I.D, *supra.*

law.[128] 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 U.S. court should look to both the law of the rendering country and U.S. law. Specifically, 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."[129] 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;

128. For a comprehensive discussion of this question, *see* Monestier, *supra* note 43.

129. RESTATEMENT (THIRD), *supra* note 45, § 482(1)(b) (emphasis added).

> (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.[130]

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."[131]

---

130. *Id.* § 421(2).

131. *Id.* § 421(3).

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, suggests that only U.S. law governs the question of personal jurisdiction. Its rule makes no mention of the rendering country'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 U.S. Constitution."[132]

Both the 1962 and 2005 Recognition Acts also prohibit a U.S. court from recognizing a judgment rendered by a foreign court that lacked personal jurisdiction over the defendant.[133] 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

132. RESTATEMENT (FOURTH), *supra* note 46, § 483(b) and cmt. e.

133. 1962 Recognition Act, *supra* note 49, § 4(a)(2); 2005 Recognition Act, *supra* note 50 § 4(b)(2).

> 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] arising out of business done by the defendant through that office in the foreign country[.][134]

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.[135] 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,"

---

134. *Id.* § 5(a).

135. Monestier, *supra* note 43, at 1743–63.

"permitted," or consistent with a "minimum contacts" analysis.[136]

Without opining on the usefulness of an inquiry into the foreign country'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 Data Protection Authority's exercise of personal jurisdiction over a U.S. defendant.

1. 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.[137]

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:

---

136. *Id.* at 1759–60.

137. GDPR, *supra* note 1, art. 3.1.

- 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.
- 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 3.1 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.[138]

138. 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*.

2. Personal jurisdiction under Article 3.2

GDPR Article 3.2, by contrast, may prove more difficult as a ground for personal jurisdiction over a U.S.-based defendant, because neither of its grounds for application of GDPR depends on 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.[139]

As an illustrative scenario in which the issue of personal jurisdiction could be especially relevant, consider a U.S.-based retailer operating a website clearly and unambiguously marketing the sales of goods or services to EU residents, but otherwise having no physical presence or stable relationships in the EU. Under the Recognition Acts, the retailer could argue 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.

---

139. GDPR, *supra* note 1, 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 defendant might have an even better chance at mounting a successful challenge to personal jurisdiction where the EU's assertion of jurisdiction over that defendant arose under GDPR Article 3.2(b) based solely on the "monitoring of behavior" of data subjects within the EU. Take, for example, a scenario contemplated by the EDPB in its Guidelines on the Territorial Scope of the GDPR, in which a U.S. company (acting as a controller) develops a health and lifestyle app that allows users to record detailed health and fitness information, and monitors the behavior of individuals in the EU who use that app.[140] For purposes of data storage, that company engages a processor—a cloud service provider—established in the U.S.[141] The EDPB concludes that in this scenario, the controller is subject to GDPR under Article 3.2, but also that the *cloud service provider* is subject to GDPR under Article 3.2 because it is engaging in

140. Territorial Scope Guidelines, *supra* note 3, at 21.

141. *Id*.

processing—data storage—that is "related to" the targeting of individuals in the EU by the controller.[142]

In the hypothetical, the cloud provider would not likely satisfy any 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. The cloud provider could thus argue convincingly that any judgment or order obtained against it in the EU related to the processing performed on behalf of the health and lifestyle app company is subject to mandatory nonrecognition under the Recognition Acts and the common law.

3. Data Protection Officers 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. 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.[143]

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.

---

142. *Id*.

143. *See* RESTATEMENT (THIRD), *supra* note 45, § 481, Reporter's Note 3; § 482, cmt. c.

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."[144] Arguably, this could be seen as either the explicit or implied 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."[145] 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.

It thus seems likely that a U.S. business that has appointed a representative under Article 27 will be found to have consented to the personal jurisdiction of the EU courts and regulators. More difficult situations would involve U.S. businesses that fail to appoint an EU representative, whether because they do not know they are obligated to do so, incorrectly determine they are not obligated to do so, or deliberately refuse to appoint an EU representative in a purposeful attempt to avoid enforcement. Under such circumstances, the U.S. court would need to determine if the U.S. entity was subject to the EU's long-arm jurisdiction despite the failure to appoint. In any case, the court's

144. GDPR, *supra* note 1, art. 27.4.

145. *Id.*, art. 27.5.

decision would likely turn on the particular facts and circumstances presented in the evidence.

A U.S. organization's appointment of a DPO under GDPR Article 37 might also lead a U.S. court to conclude that the organization consents to jurisdiction in the EU. Among the responsibilities of a DPO designated under GDPR Article 37 is that she "cooperate with the supervisory authority," "act as the contact point with the supervisory authority on issues relating to processing," and 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."[146] 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.

4. Execution of data processing and data transfer agreements: impact on personal jurisdiction in the EU

A U.S. organization could also make itself subject to a presumptively reasonable exercise of personal jurisdiction in the EU by entering into data processing or data transfer agreements with EU-based organizations in which the U.S. organization consents to such jurisdiction. To that end, both the Restatement (Third) of Foreign Relations Law[147] and the 2005 Recognition Act[148] provide grounds for a U.S. court to find that an EU court validly exercised jurisdiction over a defendant when that

146. *Id.*, arts. 38.4, 39.1(d)-(e).

147. *See* RESTATEMENT (THIRD), *supra* note 45, § 482(2)(g).

148. 2005 Recognition Act, *supra* note 50, § 5(a)(3).

defendant previously agreed to submit to the jurisdiction of the foreign court.

U.S. organizations that sign data processing and data transfer agreements that include EU Commission-approved standard contractual clauses to facilitate transatlantic data transfers may waive—at least in part—any defense based on lack of personal jurisdiction in the EU on this basis. In that regard, both the controller-to-controller and controller-to-processor versions of the standard contractual clauses give data subjects the right to enforce certain clauses against the data importer as third-party beneficiaries.[149] The clauses provide in turn that the data importer agrees to accept jurisdiction in the data exporter's country of establishment with respect to claims by data subjects in that capacity.[150]

A proposed new set of standard contractual clauses released by the European Commission in November 2020 go even further: in this new proposed set of clauses, the data importer "agrees to submit itself to the jurisdiction of the competent supervisory authority in any procedures aimed at ensuring compliance with these clauses," including inquiries and audits.[151]

---

149. *See* Commission Decision 2010/87 on standard contractual clauses for the transfer of personal data to processors established in third countries under directive 95/46/EC of the European Parliament and of the Council, 2010 O.J. L (39/5), Annex Standard Contractual Clauses, cl. 3.1; Commission Decision 2004/915/EC amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, 2004 O.J. L (385/74), Annex Set II, cl. III(b).

150. *Id*.

151. *See* 12 November 2020 Draft Annex to the Commission Implementing Decision on Standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, cl. 9(b), *available at* https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-

These draft clauses also provide that the parties "agree to submit themselves to the jurisdiction of [the] courts" of an EU member state specified by the parties.[152] If and when these clauses are approved by the EU Commission, any U.S. organization that signs them may have difficulty successfully asserting lack of personal jurisdiction in the EU as a basis for nonrecognition of a GDPR order or judgment.

B. 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.[153] "Repugnancy," however, is a stringent standard.[154] 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."[155] But although repugnancy

---

Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.

152. *Id.* cl. 3(a).

153. RESTATEMENT (THIRD), *supra* note 45, § 482(2)(d); RESTATEMENT (FOURTH), *supra* note 46, § 484(c); 1962 Recognition Act, *supra* note 49, § 4(b)(3); 2005 Recognition Act, *supra* note 50, § 4(c)(3).

154. RESTATEMENT (FOURTH), *supra* note 46, § 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.").

155. *See, e.g.*, Ohno v. Yasuma, 723 F.3d 984, 1002 (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 v. Standard Oil Co. of N.Y., 120

presents a high bar, there are several examples of cases in which courts have repugnancy as the basis for nonrecognition of foreign judgments.[156]

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 of the U.S. Constitution. One such example 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 an impermissible prior restraint on publication.[157]

N.E. 198, 201 (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.").

156. *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, 107 Cal. Rptr. 540 (Cal. 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).

157. *See* Near v. Minnesota *ex rel.* Olson, 283 U.S. 697, 716 (1931) ("[L]iberty of the press, historically considered and taken up by the Federal Constitution, has meant, principally although not exclusively, immunity from previous restraints or censorship"); Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963) ("Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity."); *See also* Kurt Wimmer, *Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers?*, 68 SYR. L.R. 547, 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

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 U.S. 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 U.S. companies abroad.[158]

In addition to First Amendment issues, GDPR orders and judgments could also raise procedural due-process concerns under the Fifth and Fourteenth Amendments of the U.S. Constitution, depending on the procedures used in the EU to issue or obtain them.[159]

Enduring and Established Constitutional Heritage (SPEECH) Act, 28 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 U.S. 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 U.S. companies abroad. *See* Wimmer at 574–75.

158. *See id*.

159. *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 U.S. courts).

VI. ALTERNATIVE ROUTES TO GDPR ENFORCEMENT IN U.S. COURTS: THE FEDERAL TRADE COMMISSION 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 GPDR judgments or orders. This part of the *Commentary* discusses two significant possibilities in that regard: (1) enforcement by the U.S. Federal Trade Commission of GDPR-related promises under its authority to police unfair and deceptive acts and practices under Section 5 of the FTC Act; and (2) contract-based actions arising out of agreements that U.S.-based organizations enter for GDPR-related purposes.

A. The Federal Trade Commission: Section 5 of the FTC Act and Privacy Shield remedies

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.[160] FTC has used that authority repeatedly to bring enforcement actions against companies that fail to abide by the commitments they make in privacy policies and other public statements about their privacy practices.[161] The FTC does not, however, have any power either to enforce non-U.S. laws or to

160. 15 U.S.C. § 45(a)(1).

161. *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 628–30 (2014).

bring actions on behalf of individual private persons who may have suffered a privacy or data-breach-related injury.

The FTC's Section 5 authority could nevertheless be used to police a U.S. company's compliance with GDPR, to the extent that company makes broad promises about GDPR compliance that extend to U.S. customers. To that end, in 2018 a representative from the agency explained that "[i]f a company chooses to implement some or all of GDPR across their entire operations, and as a result makes promises to U.S. consumers about their specific practices," then the company must live up to those commitments, as "the FTC could initiate an enforcement action if the company does not comply with" its GDPR-related promises with respect to U.S. consumers.[162]

Section 5 of the FTC Act therefore offers a potential alternative route to enforce GDPR against U.S. companies, albeit only with respect to failures to comply with GDPR-related promises made to U.S. consumers.

Notably, the FTC's authority under Section 5 of the FTC Act also includes the authority to enforce commitments made by U.S. companies that have certified to the EU-U.S. Privacy Shield program. Notwithstanding the Court of Justice of the European Union's judgment in the so-called "Schrems II" decision, which invalidated the European Commission's decision on the adequacy of the Privacy Shield program,[163] the FTC's enforcement

---

162. Daniel R. Stoller, *FTC Could Police U.S. Companies' Promises on EU Data Privacy Law,* BLOOMBERG LAW (June 20, 2018), https://bnanews.bna.com/privacy-and-data-security/ftc-could-police-us-companies-promises-on-eu-data-privacy-law.

163. *See* Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, July 16, 2020 E.C.J., *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9710189.

authority remains in place over Privacy Shield program participants who previously received personal data of EU data subjects through the program. To that end, in the wake of the *Schrems II* decision, U.S. Secretary of Commerce Wilbur Ross issued a statement indicating that the Department of Commerce would continue to administer the Privacy Shield program, and that the *Schrems II* decision "does not relieve participating organizations of their Privacy Shield obligations."[164] Thus, any U.S. organization that remains certified to the EU-US Privacy Shield program and continues to process data received under the program faces a risk of FTC enforcement if it fails to adhere to its commitments.

Such an organization could also face claims by data subjects in the EU. Specifically, Annex I to the 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.[165] 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

164. Press Release, U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows (July 16, 2020), *available at* https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and.

165. *See* Commission Implementing Decision of July 12, 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield, 2016 O.J. (L 207/1), Annex 2 Arbitral Model, Annex I.

ensuing arbitration may be conducted over the telephone.[166] Although the arbitration panel lacks any authority to grant monetary remedies to data subjects, it has the authority to impose nonmonetary relief such as granting access, correction, deletion, or return of the personal data in question.[167] 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.[168] 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.

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 of internet browser tracking mechanisms and one-off online transactions. Still others occupy a middle space: ongoing relationships of a nonessential 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 Software as a Service (SaaS). These agreements often contain a hyperlink to a "privacy policy" that has been "incorporated by reference" to the agreement and sets

166. *Id*.

167. *Id*.

168. *Id.*, Annex II § II.1.a.xi.

out the nonnegotiable terms for processing personal data that are difficult to understand by even the most experienced attorneys.

An EU data subject who has established a contractual relationship with a U.S.-based controller that includes data protection provisions, depending on the contract's choice-of-forum provisions, might thus be able to seek enforcement of her rights in a breach-of contract action filed directly against the controller in a U.S. court.

2. Contracts between data controllers and data processors under GDPR Article 28

Under GDPR Article 28, when a controller engages a processor, the parties are obligated to enter into a contract that governs the processing, is "binding on the processor with regard to the controller," and includes various mandatory terms relating to the processing.[169] The processor is in turn obligated to impose the same obligations on any other processors it engages to carry out that processing.[170]

When a U.S.-based processor signs a contract pursuant to Article 28 with an EU-based controller or processor, that contract provides another means through which the GDPR's requirements might be enforced against the U.S.-based processor. If the U.S.-based processor violates the requirements of the processing agreement, the EU-based controller or processor can—depending on the contract's choice of forum—enforce that contract directly against the U.S.-based processor in a U.S. court.

169. GDPR, *supra* note 1, art. 28.3.

170. *Id.* at art. 28.4.

3. Data transfer contracts based on Standard Contractual Clauses

As noted in Part V.A.4 above, U.S. organizations acting as controllers or processors may also enter into data processing and data transfer agreements that incorporate standard contractual clauses approved by the EU Commission to address GDPR's restrictions on cross-border data transfers.[171]

An EU data exporter with whom the U.S. organization has executed the standard contractual clauses, or a data subject with status as a third-party beneficiary under those clauses,[172] could bring an action to enforce the clauses against the U.S. organization in a U.S. court.

171. *See id.* art. 46.2(c).

172. *See* Commission Decision 2010/87 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, 2010 O.J. L (39/5), Annex Standard Contractual Clauses, cl. 3; Commission Decision 2004/915/EC amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, 2004 O.J. L (385/74), Annex Set II, cl. III(b).

VII. CONCLUSION

Since its entry into force, GDPR has given rise to important questions about the reach of European data protection rules, and the ability of individuals and supervisory authorities to enforce those rules against foreign defendants. The answers to those questions can be especially complex for U.S.-based organizations that do not maintain a physical presence or other assets in the EU, but still fall within GDPR's extraterritorial reach. The *Commentary* discusses whether and how a party in the EU—whether a supervisory authority, individual data subject, or not-for-profit body acting on behalf of data subjects—can obtain such an organization's compliance with GDPR through resort to a U.S. court proceeding.

The *Commentary* outlines the considerations, both legal and practical, that U.S.-based organizations and parties in the EU should consider when faced with the question of how a U.S. court might address a request to enforce a GDPR order or judgment. As the *Commentary* shows, the enforceability of GDPR orders and judgments in a U.S. court will depend on several factors, including the nature of the relief sought through the order or judgment, the nature of the underlying violation and the process through which the order or judgment was initially obtained in the EU, and the U.S. organization's contacts with the EU. By exploring how those factors might influence a court's application of the existing body of U.S. law regarding the recognition and enforcement of foreign judgments, the *Commentary* provides a framework that parties on both sides of the Atlantic can use to evaluate whether, in a given case, the long arm of the GDPR might reach a U.S. defendant.