August 10, 2020

GDPR Issues In International Arbitration

The European Union's ("EU") General Data Protection Regulation ("GDPR") came into effect in May 2018, and its broad applicability has raised significant as-yet unanswered questions for practitioners of international arbitration, including whether and how the GDPR applies in that forum.[1] The recent Court of Justice of the European Union ("CJEU") decision invalidating reliance on the EU-U.S. Privacy Shield Framework will only serve to heighten concerns about how to navigate GDPR issues in connection with international arbitration.[2]

The GDPR was adopted by the EU to harmonize data privacy laws across the EU Member States and to provide greater protection and rights to data subjects. As the GDPR permits significant fines for breaches of its protocols, including up to the greater of €20 million or 4% of a company's global annual revenue,[3] practitioners and business leaders are rightly concerned about compliance. Given the cross-border nature of international arbitration and the inevitable data-sharing obligations inherent in disclosure and fact-finding processes, the GDPR may have significant impact on the process of international arbitration. Arbitral institutions therefore have a significant opportunity to improve the effectiveness and appeal of international arbitration by developing clear guidance on the applicability of the GDPR to prevent disputes from arising among participants down the line. Many arbitral institutions are addressing the GDPR in new guidance and rules to ensure both that there is a consistency in approach and that concerns about GDPR compliance do not interfere with the arbitration.

This memorandum discusses issues that arise under the GDPR in international arbitration, recent developments and rules adopted to address the GDPR in arbitration, and how parties in an international arbitration can manage the risks of GDPR compliance in the absence of clear guidance from the tribunal.

Applicability of the GDPR to International Arbitration

The Scope of the GDPR

As an initial matter, parties engaged in international arbitration must determine whether the GDPR applies to their proceeding. The GDPR's broad definition of "processing" data and its wider territorial reach mean that the GDPR can apply to various arbitral participants involved in the disclosure or fact-finding process—including a party, counsel, the arbitrator, a witness, an expert, a document custodian, and a third party vendor—if a participant or "data subject" is subject to the GDPR's protections.[4]

The GDPR sets forth several principles for personal data processing that may be relevant to international arbitration. It requires that personal data be collected for specified and legitimate purposes and processed

lawfully, transparently, and securely. Furthermore, the personal data must be accurate and adequate, and be kept no longer than necessary.[5]

Processing of personal data is lawful under the GDPR only when conducted in line with one of the enumerated legal bases provided in the regulation; however, it is unclear the extent to which any of these legal bases apply to international arbitration. For example, the GDPR permits a party to process personal data if "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party,"[6] which may potentially be cited by arbitral participants as an applicable legal basis for processing relevant personal data, although there is limited guidance on this topic.

In addition, the GDPR permits personal data processing if it is "necessary for compliance with a legal obligation to which the controller is subject"; however, the regulation requires that the legal obligation be imposed by the EU or Member State law.[7] That leaves open the question whether an obligation established by an international arbitration tribunal is imposed by the EU or Member State law either because the tribunal's powers are in some sense governed by EU law or because the arbitration is pursuant to a treaty involving the EU or a Member State. Therefore, it is unclear whether international arbitration practitioners can rely on this legal basis to process personal data.

GDPR Rules of Data Transfer

The GDPR's requirements on transferring personal data to a third country outside the EU also bear particular relevance to international arbitration, where the need to transfer data from an EU country to a non-EU country frequently arises. Under the GDPR, transfer of personal data to a non-EU country is prohibited unless one of the following conditions are met: (1) the European Commission ("EC") has determined that the destination country provides an adequate level of protection;[8] (2) the data controller or processor has provided appropriate safeguards—such as binding corporate rules and standard data protection clauses—with enforceable data subject rights and effective legal remedies for data subjects;[9] or (3) the one-off transfer meets one of the few enumerated derogations, or exceptions.[10] One of the exceptions the GDPR carves out allows transfer if it "is necessary for the establishment, exercise or defence of legal claims,"[11] which would seem to apply to international arbitration. However, derogations are not intended as a means to legitimize systematic or continual data transfer.

Notably, under the GDPR, a transfer ordered by an arbitral tribunal in a non-EU third country—such as a document production order—is only enforceable if, "based on an international agreement, such as a mutual legal assistance treaty" between the third country and the EU or Member State.[12] Therefore, without a qualifying treaty, parties may not be able to rely merely on an order from a non-EU tribunal to transfer personal data outside the EU.

Notwithstanding these provisions, the applicability of the GDPR is not always clear. In *Tennant Energy, LLC (U.S.A.)* v. *Gov't of Canada*, an international arbitration under NAFTA, the tribunal held that the

GDPR did not apply to the arbitration because "neither the EU nor its Member States are party" to NAFTA.[13] This decision was particularly interesting because one of the three arbitrators was a barrister in the United Kingdom, which was then still a member of the EU.[14]

Ultimately, the applicability of the GDPR to an international arbitration will depend on the facts and circumstances of the case, the applicable rules of the tribunal, and (perhaps) the whims of arbitrators.

Responses by Arbitral Organizations

Although the applicability of the GDPR to international arbitration remains uncertain, several arbitral organizations have created rules to align their practices with the strictures of international data privacy regimes like the GDPR. In January 2019, the International Chamber of Commerce ("ICC") added new rules concerning Protection of Personal Data.[15] The updated ICC rules expressly "recognise[] the importance of effective and meaningful personal data protections when [the ICC] collects and uses such personal data as data controller pursuant to data protection regulations, including the [GDPR]."[16] Moreover, the new rules ask parties to ensure that they comply with the GDPR and ask arbitral tribunals to remind "party representatives, witnesses, experts and any other individuals appearing before it that the GDPR applies to the arbitration."[17] This often will take the form of a data protection protocol to be created by all participants, including members of the tribunal. In December 2019, the London Court of International Arbitration ("LCIA") also indicated in its online New Year's greeting that it would update its rules in 2020 to include "wording on . . . GDPR."[18]

Professional organizations have also turned their attention to addressing the challenges posed by the GDPR in international arbitration. The International Council for Commercial Arbitration ("ICCA") and the International Bar Association ("IBA") have established a Joint Task Force on Data Protection in International Arbitration Proceedings to produce a comprehensive guide to data protection in international arbitration. The Joint Task Force has released a consultation draft of its guide, *ICCA-IBA Roadmap to Data Protection in International Arbitration*, which is heavily focused on the GDPR.[19] Similarly, a working group of The Sedona Conference, a leading voice on electronic discovery and data privacy, is currently drafting a new commentary, "The Sedona Conference Arbitration Principles," which will address data privacy and security issues in international arbitration.

Potential Risks Involving GDPR Compliance

The most obvious risk involving the application of the GDPR in international arbitration is the potential for financial penalties for violating its broad strictures. Violation of certain GDPR provisions can result in fines as much as €20 million or up to 4% of the company's global annual turnover of the preceding financial year, whichever is higher. Failure to comply with provisions on international personal data transfer and lawful personal data processing can subject a party to the maximum fine.[20] Moreover, a party may be subject to

financial penalty for another party's violation, as the GDPR imposes joint liabilities on joint data controllers.[21]

It is also noteworthy that the restrictions on international data transfer apply not only to the initial transfer from the EU to a third country, but also to the onward transfer from the recipient third country to another third country.[22] Therefore, in an international arbitration, parties and other participants must ensure compliance with these provisions when they transfer personal data originally received from the EU onward to another non-EU country, such as when a party submits evidence received from a witness in the EU to a non-EU tribunal.

A less obvious, but no less critical risk raised by the GDPR in international arbitration is the potential for its abuse. Parties may use the GDPR as a shield to prevent the disclosure of important information—without making a good faith effort to make the disclosure possible—in the course of an international arbitration. For instance, a party may object to disclosure requested by the opposing party on the ground that those documents contain personal data unrelated to the claims being arbitrated and, therefore, cannot be transferred to a non-EU country in accordance with the GDPR.[23] A party may also argue that redacting the personal data is unduly burdensome and disproportionate to the need of the arbitration, and ask the tribunal to prohibit disclosure. Such efforts, if not checked by the tribunal, may lead to delay and satellite hearings on disclosure, and may make international arbitration less attractive.

Similar arguments have been advanced in the context of litigation in the U.S.[24] More often than not, U.S. courts reject such arguments and order disclosure.[25] International arbitral tribunals may hold a different view.

Managing the Risks of GDPR Compliance

In light of the broad reach of the GDPR, parties in an international arbitration may want to contemplate how to manage the risks of complying with the GDPR as soon as they decide to initiate the arbitration proceeding. Absent specific guidance—like that from the ICC—at the very outset, parties are encouraged to carefully assess whether the GDPR applies or may apply to them, taking into consideration the location of potential arbitrators, fact and expert witnesses, and third-party vendors—such as e-disclosure vendors and translators—that they may need to engage. The assessment may remain an ongoing process, as new players and information are added as the arbitration proceeds. If parties cannot agree on the applicability of the GDPR, they may raise the issue with the tribunal.

After a determination regarding the applicability of the GDPR is reached, parties may work together to develop a data processing and disclosure protocol. The protocol may include, among other things: (1) categories of data to be processed and disclosed during the course of the arbitration, and the purpose and legal basis for such processing and disclosure; (2) categories of data subjects and procedures to notify those data subjects of the processing of their personal data (if required); (3) whether transfer to a non-EU

third country will occur and the legal basis for such transfer; (4) techniques to facilitate data minimization; (5) safeguards to ensure data security and confidentiality; (6) data retention and purging procedures at the conclusion of the proceeding; and (7) how parties and other data controllers will oversee compliance with data protection regulations. If the parties cannot agree on any terms of the protocol, they may raise the issues with the tribunal. Parties face increased risks if they process data governed by the GDPR without a protocol in place

Even if parties determine that they are not governed by the GDPR upon initial assessment, they are still encouraged to adopt the forgoing approach to minimize the risk of future non-compliance with the GDPR and to address the equally important data security and confidentiality concerns that arise even when the GDPR is not applicable. Given the broad reach of the GDPR, the potential penalties for violation, the uncertainties in its application in international arbitration, and the possibility of subsequently implicating the GDPR during the course of the arbitration, it is prudent for parties to comply with the GDPR's requirements to the extent that they do not unduly interfere with or substantially burden the arbitration.

Conclusion

The GDPR's broad reach, the complexity and comprehensiveness of its terms, and the risks of non-compliance warrant heightened attention from parties in international arbitration. Parties should be mindful of data protection issues raised by the GDPR throughout the proceeding, and are encouraged to take timely and effective measures to minimize the risks of non-compliance.

In addition, arbitral institutions have an opportunity to develop clear guidance on data privacy and security to allow an arbitration to proceed efficiently through a hearing (particularly in a post-COVID-19 world in which many courts are closed). In particular, arbitral institutions should consider taking steps to make sure that litigants are not able to weaponize the protections of the GDPR during the disclosure process. It is worth noting that while efforts ensuring GDPR compliance may require some initial commitment of time and resources, it should not be seen as a restriction to an effective arbitration and certainly should not deter parties from engaging in the proceeding. In fact, many principles promulgated by the GDPR—such as data minimization, efficiency, and security—are consistent with the key features of international arbitration and, therefore, should not impede effective dispute resolution through arbitration.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Allan J. Arffa
+1-212-373-3203
aarffa@paulweiss.com

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Jessica S. Carey
+1-212-373-3566
jcarey@paulweiss.com

Geoffrey R. Chepiga
+1-212-373-3421
gchepiga@paulweiss.com

Christopher D. Frey
+81-3-3597-6309
cfrey@paulweiss.com

Aidan Synnott
+1-212-373-3213
asynnott@paulweiss.com

Associates Carter Greenbaum and Sylvia Sui contributed to this Client Memorandum.

---

1 We have previously published a client memorandum on the key provisions and implications of the General Data Protection Regulation ("GDPR"), *available* here.

2 We have previously published a client memorandum on the CJEU decision, *available* here.

3 GDPR Art. 83.

4 The GDPR defines personal data as "any information relating to an identified or identifiable natural person ('data subject')." GDPR Art. 4. Data processing includes "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." *Id.* The GDPR applies to the processing of personal data (1) "in the context of the activities of an establishment of a controller or a processor in the [European] Union, regardless of whether the processing takes place in the [European] Union or not[,]" or (2) "of data subjects who are in the [European] Union by a controller or processor not established in the [European] Union, where the processing activities are related to . . . the offering of goods or services . . . to such data subjects in the [European] Union . . . [or] the monitoring of their behavior as far as their behavior takes place within the [European] Union. GDPR Art. 3.

5 GDPR Art. 5.

6 GDPR Art. 6.

7 *Id.*

8 GDPR Art. 45.

9 GDPR Art. 46.

10 GDPR Art. 49.

11 *Id.*

[12] GDPR Art. 48; GDPR Rec. 115.

[13] *Tennant Energy, LLC (U.S.A.)* v. *Gov't of Canada*, PCA Case No. 2018-54, Tribunal's Comm. to the Parties (Jun. 24, 2019), *available* here.

[14] *Tennant Energy, LLC (U.S.A.)* v. *Gov't of Canada*, PCA Case No. 2018-54, Claimant's E-mail to the Tribunal regarding the Application of the EU GDPR (Apr. 17, 2019), *available* here.

[15] *See* Int'l Chamber of Com., ICC Note to Parties and Arbitral Tribunals on the Conduct of the Arb. Under the ICC Rules of Arb., ¶¶ 80–91, *available* here.

[16] *Id.* at ¶ 80.

[17] *Id.* at ¶¶ 83–84.

[18] London Ct. of Int'l Arb. ("LCIA"), *Season's Greetings from the LCIA* (Dec. 19, 2019), *available* here.

[19] *See* ICCA-IBA Joint Task Force on Data Protection in Int'l Arb., *ICCA-IBA Roadmap to Data Protection in Int'l Arb*. (Feb. 2020), *available* here.

[20] GDPR Art. 83.

[21] GDPR Art. 26. Joint controllers are defined as controllers who "jointly determine the purposes and means of processing." *Id.*

[22] GDPR Art. 44.

[23] *See* GDPR Art. 49 (transfer of personal data to non-EU third country allowed if "necessary for the establishment, exercise or defence of legal claims").

[24] *See, e.g.*, *SEC* v. *Telegram Grp. Inc.,* No. 19 CIV. 9439, Letter from Defs. to Judge P. Kevin Castel, Dkt. No. 62 (S.D.N.Y. Jan. 9, 2020); *In re Mercedes-Benz Emissions Litig*., No. 16-CV-881, 2020 WL 487288, at *4 (D.N.J. Jan. 30, 2020).

[25] *See, e.g.*, *SEC* v. *Telegram Grp. Inc.,* No. 19 CIV. 9439, Order, Dkt. No. 67 (S.D.N.Y. Jan. 13, 2020); *In re Mercedes-Benz Emissions Litig*., No. 16-CV-881, 2020 WL 487288, at *8 (D.N.J. Jan. 30, 2020).