Fordham International Law Journal

Volume 41, *Issue* 4 2018 *Article* 4

2017 FORDHAM INTERNATIONAL ARBITRATION & MEDIATION CONFERENCE ISSUE

It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration

Kathleen Paisley*

*

ARTICLE

IT'S ALL ABOUT THE DATA:

THE IMPACT OF THE EU GENERAL DATA PROTECTION REGULATION ON INTERNATIONAL ARBITRATION

Kathleen Paisley[*]

ABSTRACT

This Article addresses the application of the EU General Data Protection Regulation (GDPR) to international commercial arbitration. The GDPR has a broad reach and where applicable imposes significant obligations on the processing of personal data during arbitrations. The GDPR imposes potential criminal liability and fines of up to the higher of 4% of global gross revenue or EU €20 *million, as well as granting data subject's individual rights of action for damages, which means the risks of non-compliance are steep.*

The GDPR covers all data custodians with an EU establishment or that target EU data subjects, including the parties, their counsel, arbitral institutions, members of the arbitral tribunal, experts and vendors, each of whom has individual liability for GDPR compliance. Furthermore, the purposefully broad definitions of what constitutes both personal data and data processing mean that literally all arbitral activities involving data that either identifies or could identify an individual are likely to be caught by the regulation (including evidence (e.g., emails, contracts, lab notebooks, construction logs), memorials, witness statements, expert reports, and the award itself).

---

* Kathleen Paisley, www.amboslaw.be, a U.S. national, is a New York and DC qualified international arbitrator, mediator, and counsel, with extensive experience in IP, technology and data, including providing expertise concerning the complex data and technology issues affecting international arbitration, as well as finance, accounting, and damages issues. She is based in Brussels, and splits her time with New York, London, and Miami. (JD (Yale, 1986), CPA exam (Florida, 1986), MBA, Finance (FAU, 1984), BS, (FSU, 1981)).

The GDPR prohibits the processing of personal data and its transfer outside the European Union, including during an arbitration, except under certain limited conditions. When personal data processing is permitted, it must be undertaken in a manner that is legitimate, fair and transparent, data minimization and adequate cybersecurity measures are required, and data retention is circumscribed. The GDPR also grants other significant rights to data subjects, which includes anyone identifiable from a document or the evidence, including the right to transparent information (which may include data privacy notices) and to review and to rectify data, among other things. This could cover literally hundreds of individuals in a complex case.

Needless to say, reconciling these broad-ranging rights and obligations with the cross-border, consensual, decision-making function of international arbitration will be challenging, whereas EU courts are largely exempt from the GDPR. This is further complicated by the fact that the GDPR's most strenuous obligations fall on "controllers" of data, which is defined in a manner that includes virtually everyone involved in an arbitration, thereby creating overlapping and potentially conflicting obligations with corresponding liability attaching to each.

This Article reviews the GDPR's legal framework as it applies to international commercial arbitration, and its practical application to the arbitral process. The Author stresses the importance of addressing data protection early through the adoption of a data protection protocol or other measure to address compliance, and considers the GDPR's potential impact on data disclosure. Furthermore, given the complexities and the significant risk, the Author suggests that the international arbitration community should consider creating increased certainty by proactively addressing the application of the GDPR to international arbitration with the relevant regulators to develop an agreed framework for GDPR compliance within the arbitral process.

I. INTRODUCTION

Data processing is an essential component of modern international arbitration. The confluence of three factors over the last two decades has changed (or will change) international arbitration: (1) globalization has caused a dramatic increase in the importance of international commercial arbitration as a dispute settlement mechanism; (2) digitalization has created a significant increase in the amount and complexity of data processed during a typical international commercial arbitration; and (3) led by the European Union[1] the data protection laws potentially applicable to that data have proliferated and, with the adoption of the EU General Data Protection Regulation ("GDPR"),[2] have become key compliance imperatives. The result is that access to, and processing of, digital data is key to the efficient and effective resolution of complex commercial disputes through international arbitration.[3] Therefore, while international commercial arbitration's function remains to decide disputes according to a binding and often confidential process

1. The current twenty-eight EU Member States are: Austria, Belgium, Bulgaria, Cyprus, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the Netherlands and the United Kingdom. *EU Member Countries in Brief*, EUROPEAN UNION, https://europa.eu/european-union/about-eu/countries/member-countries_en (last updated Mar. 18, 2018). The General Data Protection Regulation ("GDPR") will initially apply to the European Union and will then be implemented into the Agreement on the European Economic Area (the "EEA Agreement") at which point its application will be extended to the entire European Economic Area ("EEA"). The EEA Agreement encompasses the 28 EU Member States and the three EEA EFTA states (Iceland, Liechtenstein and Norway), establishing an internal market governed by the same basic rules regarding free movement of goods, services, persons and capital. EU acts such as the GDPR that are deemed to be EEA Relevant are incorporated into the EEA Agreement. A draft Joint Committee Decision (JCD) is under consideration by the European Union and the EEA EFTA States with the goal that the GDPR will be incorporated into the EEA Agreement on June 1, 2018. See *Incorporation of the GDPR into the EEA Agreement*, EUROPEAN FREE TRADE ASSOCIATION (Apr. 13, 2018). http://www.efta.int/EEA/news/Incorporation-GDPR-EEA-Agreement-508041 [https://perma.cc/V8XC-262J] (archived Apr. 27, 2018). Therefore, all references in this Article to "European Union" or "EU" should be read to include the 31 EEA countries after implementation of the GDPR into the EEA Agreement is completed. The Article was finalized in May 2018, and the information is current as of that date.

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

3. This Article is focused solely on international commercial arbitration, although the principles addressed herein impact investor-State arbitration and domestic arbitration when EU personal data is processed therein.

agreed to by the parties, it has also become a data management exercise requiring data to be processed, often across borders, and requiring compliance with relevant data protection laws, including the GDPR.

While many of these laws have been in place for decades, this issue is currently coming to the fore because an increasing number of entities both within and without the European Union are subject to EU-style data protection obligations and, at least in the case of the GDPR, the risk of noncompliance has become significant and is expected to take a seat in the board room alongside antitrust and anticorruption.[4] This has been aptly referred to by a leading EU data protection expert as the "Brussels Effect,"[5] and has led Fortune 500 companies to spend an estimated EU€8 billion in efforts to comply with the GDPR even before it has come into effect.[6] However, Brussels Effect notwithstanding, at the moment there is very little dialogue between the data protection and international arbitration communities. The application of the data protection laws to the taking of evidence in international arbitration is not expressly addressed by the highly influential 2010 International Bar Association Rules on the Taking of Evidence in International Arbitration ("IBA Rules") nor any of the protocols that address the exchange of evidence in international arbitration.[7] Furthermore, while the principles contained in the GDPR apply to arbitration, the GDPR does not directly address how it is to be applied to arbitration, which has created significant

4. *See* Mark Scott & Laurens Cerulus, *Europe's New Data Protection Rules Export Privacy Standards Worldwide*, POLITICO (Jan. 31, 2018, 12:00 PM), https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/ [https://perma.cc/6FT8-BM3T] (archived Mar. 19, 2018) [hereinafter Scott & Cerulus].

5. *Id.* (referencing a conversation with Christopher Kuner, co-chair of the Brussels Privacy Hub at the Vrije Universiteit Brussel).

6. *See* Mehreen Khan, *Companies Face High Cost to Meet New EU Data Protection Rules*, FINANCIAL TIMES (Nov. 19, 2017), https://www.ft.com/content/0d47ffe4-ccb6-11e7-b781-794ce08b24dc.

7. *See generally* IBA RULES ON THE TAKING OF EVIDENCE IN INT'L ARBITRATION (INT'L BAR ASS'N, 2010) [hereinafter IBA RULES]; ICDR GUIDELINES FOR INFORMATION DISCLOSURE AND EXCHANGE IN INTERNATIONAL ARBITRATION PROCEEDINGS (INT'L CTR. FOR DISPUTE RESOLUTION, 2008); CPR PROTOCOL ON DISCLOSURE OF DOCUMENTS AND PRESENTATION OF WITNESSES IN COMMERCIAL ARBITRATION (INT'L INST. FOR CONFLICT PREVENTION & RESOLUTION, 2008); PROTOCOL FOR E-DISCLOSURE IN INTERNATIONAL ARBITRATION (CHARTERED INST. OF ARBITRATORS, 2008).

confusion and uncertainty within the international arbitration community about what it needs to do to comply.[8]

This confusion and uncertainty is enhanced by the fact that Member States have taken different approaches to the regulation of the data that may be covered during an arbitration, leading to potentially conflicting regulatory frameworks even within the European Union.[9] The GDPR's impact on arbitration will therefore be an iterative process as data custodians covered by its terms receive further guidance from the EU institutions, Member State laws implementing the GDPR, and Member State data protection authorities. However, as the GDPR becomes effective immediately, arbitral data custodians falling within its scope will need to make a good faith attempt to apply its provisions to the arbitrations in which they are involved or risk fines and other criminal or civil sanctions.[10]

This Article addresses the impact of the GDPR on international arbitration and the custodians of the data exchanged during the arbitral process, including the parties, their counsel, arbitral institutions, counsel, members of the arbitral tribunal,[11] experts and vendors,[12] and the support staff working for each of them (referred to as "Arbitral Data Custodians"). The Article is geared at making an initial attempt to bridge the knowledge gap between international arbitration practitioners and data protection specialists.[13] It is not intended as either a treatise on international arbitration or the GDPR,

8. *See* GDPR, *supra* note 2, recital 52 at 10 (stating that special categories of data may be processed "where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure." This reference to "out-of-court procedure is used only two times in the GDPR and is not defined.)

9. *Cf.* German Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (DSAnpUG-EU) (June 30 2017) with Irish Data Protection Bill 2018 (No. 10b of 2018) [hereinafter Irish DP Bill]

10. *See generally Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679*, (Article 29 Data Protection Working Party, 17/EN WP 253, 2017) [hereinafter Guidelines on Fines]. Because the EDPB is not yet established, Working Party 29 issued these preliminary guidelines.

11. The term arbitral tribunal or tribunal is used to refer to the arbitrators who decide the case, whether it be a sole arbitrator or a panel of three.

12. Vendors may include e-discovery experts, information technology ("IT") professionals, court reporters, translation services, couriers and among others.

13. For an excellent discussion of the policy considerations underpinning the issues addressed in this article, see CHRISTOPHER KUNER & DANIEL COOPER, *DATA PROTECTION LAW AND INTERNATIONAL DISPUTE RESOLUTION*, VOLUME 382 *RECUEIL DES COURS DE L'ACADÉMIE DE DROIT INTERNATIONAL DE LA HAYE,* HAGUE ACADEMY OF INTERNATIONAL LAW (BRILL/NIJHOFF) 9-174 (2017) [hereinafter KUNER & COOPER].

but rather seeks to provide a broad understanding of how the two may work together going forward, with the caveat that at the time the Article was written, the GDPR was just coming into force and many of the laws implementing it into Member State law are yet to be finalized.

The Article begins by providing a general background to EU data protection laws, with a focus on the GDPR and the changes it brings from the Data Protection Directive ("DP Directive") previously in place.[14] The Article then describes the legal framework established by the GDPR and its potential impact on international arbitration.[15] Given the significant uncertainty about the application of the GDPR in practice, and the lack of any specific guidance on its application to arbitration, the focus is on raising the relevant questions to be considered, with the realization that the solutions to these questions are highly case and party specific and will vary depending on the nature and location of the data and the data custodians who will process it. The final section of the Article analyzes how the data protection principles found in the GDPR have the potential to affect the management of data in a complex international commercial arbitration by posing some of the relevant legal questions raised and how they are likely to be resolved based on the most relevant precedent promulgated under the previous DP Directive, again with an understanding that this is a work in progress. The principles discussed herein are applicable under the data protection laws of many countries, however, this Article focuses on the application of the GDPR because of its sweeping application and broad-ranging implications.[16]

14. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. L 281/31 [hereafter DP Directive]. For an excellent overview of European data protection law under the DP Directive, much of which carries over to the GDPR, see EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, HANDBOOK ON EUROPEAN DATA PROTECTION LAW (2014) [hereinafter EU Handbook].

15. For interesting discussions of some of the issues addressed in this article in the context of the DP Directive, see Karin Retzer & Sherman Khan, *Balancing Discovery with EU Data Protection in International Arbitration Proceedings*, 3 N.Y. DISP. RESOL. L., (Spring 2010), at 47; Markus Burianski & Martin Reindl, *Truth or Dare? The Conflict Between E-discovery in International Arbitration and German Data Protection Rules,* 2010 Zeitschrift für Schiedsverfahren [SchiedsVZ] 187, 187-200. [hereinafter Burianski & Reindl]

16. *See* Scott & Cerulus, *supra* note 4.

II. BACKGROUND TO EU DATA PROTECTION

The right to privacy was first espoused by Samuel Warren and Louis Brandeis in their seminal article aptly entitled "The Right to Privacy" published in the *Harvard Law Review* in 1890.[17] The modern era of data protection law, which is similar to, but not the same as, the right to privacy,[18] started just over two decades ago with the European Union's adoption of the DP Directive in 1995, which was recently replaced by the GDPR.[19] The DP Directive led the way for more than 100 countries (including EU Member States) to adopt data protection or privacy regimes "enshrining" an individual's rights in his or her personal data and providing data subjects with broad ranging protections and corresponding obligations.[20] Many of these laws are based in large part on the DP Directive.[21]

The DP Directive covered a very broad range of "personal data" and included detailed rules on if, and if so, when, where, and how personal data could be processed and placed obligations on data "controllers" and "processors" for compliance with its terms.[22] Although counterintuitive in a digital environment, the premise of the DP Directive (and the GDPR) is that the processing of personal data by a third party is prohibited unless expressly allowed by the GDPR. It is necessary to make this mind shift in order to understand how the GDPR operates and how it applies to international arbitration. Many of the principles established by the DP Directive are unchanged in the GDPR.[23] However, important new rights have been added (including for example the right to rectification and erasure) and significant changes have been made to the procedure by which the rules are

17. *See* Samuel Warren and Louis Brandeis, *The Right to Privacy*, 4 HARVARD L. REV. 193 (1890).

18. The right to privacy set forth by Warren and Brandies is closely related to the data protection principles set forth in the DP Directive and the GDPR and discussed in this Article, but they are not the same in that privacy focuses more on the individuals' right and data protection refers to legal rules that govern the processing of the data. *See* KUNER & COOPER, *supra* note 13, at 25.

19. *See generally* GDPR *supra* note 2; DP Directive *supra* note 14.

20. *See* KUNER & COOPER, *supra* note 13, at 33 (citing Graham Greenleaf, *Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority*, 133 PRIVACY L. & BUS. INT'L REP. (Jan. 30, 2015)).

21. *See id*. at 33.

22. *See* DP Directive, *supra* note 14 at 38-39.

23. *See generally* GDPR, *supra* note 2; DP Directive, *supra* note 14.

enforced.[24] Furthermore, the sanctions for noncompliance have been enhanced including individual rights of action by data subjects, criminal sanctions and greatly increased penalties, the largest of which apply to unlawful data transfer outside the European Union (an issue that is often raised in international arbitration).[25]

A. Change to a Regulation

The first principle to be understood about the GDPR is that it is a regulation rather than a directive and how this impacts its enforcement under EU law. As a directive, the DP Directive had to be implemented into a Member State's national law to become effective, which left significant room for differences in the Member States' implementation of certain of its provisions.[26] This led to fragmentation in how data was regulated across the European Union with resulting difficulties in compliance and concerns about digital market disruption caused by the unclear playing field.[27] Furthermore, when the DP Directive was being drafted and debated, use of the internet was in its infancy, hence its provisions were not originally drafted with a complete understanding of how they would be applied in a digital landscape.[28] Furthermore, the lack of serious fines and other adverse consequences for breach caused some to refer to the DP Directive as a "toothless tiger."[29]

In an attempt to address these and other concerns, after four years of debate and compromise, the European Union adopted the GDPR in 2016, which replaced the DP Directive on May 25, 2018.[30] As a regulation, the GDPR is a law enforceable across the European

---

24. *See* GDPR, supra note 2, arts. 16-17, at 43-44;(defining the rights of rectification and erasure); arts. 51-76, at 65-79 (describing roles and responsibilities of supervisory authorities)

25. *See id*., arts. 77-84, at 80-83 (addressing fines and penalties).

26. *See* Communication from the Commission to the European Parliament and the Council, Stronger Protection, New Opportunities – Commission Guidance on the Direct Application of the General Data Protection Regulations as of 25 May 2018, COM (2018) 43 final, at 2-3 (Jan. 24, 2018) [hereinafter 2018 Communication].

27. *See id.*

28. Public access to internet can be traced back to the release of the World Wide Web software by the European organization for Nuclear Research ("CERN") in 1993. *The Birth of the Web*, CERN, https://home.cern/topics/birth-web [https://perma.cc/M3E8-MZPC] (archived Apr. 27, 2018). The DP Directive was adopted in 1995. *See* DP Directive, *supra* note 14. The author was also directly involved in lobbying the DP Directive.

29. *See, e.g.*, Brian Mahoney, *Data Protection Law – No longer a Toothless Tiger*, GDPR Forum (2017).

30. *See* GDPR, *supra* note 2, arts. 94(1), 99, at 86-87.

Union without the need for Member State implementing legislation.[31] However, the enactment of the GDPR does not mean that the Member States will cease having data protection laws, indeed, Member States are in the process of amending their existing laws implementing the DP Directive to bring them in line with the GDPR.[32]

The GDPR also includes a number of areas where Member States are expressly allowed to derogate from its terms, and important differences have already been observed in the ways that existing Member State data protection laws are being brought into line with the GDPR.[33.] This includes the right to exempt "judicial proceedings" and "the enforcement of civil law claims" from the application of some of the more strenuous rights and obligations imposed by the GDPR provided other safeguards are put in place. [34] Some Member States, for example Ireland, have applied this exemption broadly in a manner that exempts certain types of data that is typically processed during an arbitration from these rights, although the other provisions of the GDPR remain applicable. It remains to be seen if other Member States will follow suit and whether the European Union will take a position on these exemptions.[35] The GDPR also includes a broad right to derogate with respect to employee data, which is also likely to impact international arbitration.[36]

B. Internal Compliance Requirements

The GDPR also moves away from the notification system established by the DP Directive, whereby data custodians could gain comfort from notifying their data protection operations to their local data protection authority, to a largely self-regulation system.[37] For

31. 2018 Communication, *supra* note 26, at 2-3.

32. *See* Lokke Moerel, *GDPR Conundrums: The GDPR Applicability Regime – Part 1: Controllers*, PRIVACY TRACKER (Jan. 29, 2018), https://iapp.org/news/a/gdpr-conundrums-the-gdpr-applicability-regime-part-1-controllers/ [https://perma.cc/F3A8-BSHS] (archived May 30, 2018) [hereinafter *GDPR Conundrums Part 1*]; Lokke Moerel, *GDPR Conundrums: The GDPR Applicability Regime – Part 2: Processors*, PRIVACY TRACKER (Feb. 6, 2018), https://iapp.org/news/a/gdpr-conundrums-the-gdpr-applicability-regime-part-2-processors/ [https://perma.cc/6YP9-XX27] (archived May 30, 2018).

33. *See GDPR Conundrums Part 1*, *supra* note 32.

34. *See* GDPR, *supra* note 2, art. 23 at 46—47.

35. *See* Irish DB Bill, *supra* note 9, art. 161 at 136-137.

36. GDPR, *supra* note 2, art. 88, at 84.

37. *See generally,* GDPR, *supra* note 2. This fundamental change from a notification system to one of self-regulation can broadly be analogized to the changes made to EU competition laws over the last two decades, with the European Union moving from a

entities with large and potentially risky data processing operations, this self-regulatory system requires appointing an independent and autonomous data protection officer ("DPO") to monitor compliance and others may voluntarily appoint a DPO in which case the same rules apply.[38] Formal data protection impact assessments will be required where data processing is undertaken that "is likely to result in a high risk to the rights and freedoms of natural persons."[39] Furthermore, data protection principles must be imbedded into all new data processing operations from the outset (*e.g.* data minimization) either through so-called "privacy by design" or by default to the strictest measures.[40]

To help ensure these rules are followed, the GDPR makes the data controller accountable for compliance and requires the controller to be able to "demonstrate" compliance.[41] This means keeping records of what decisions were made with respect to the protection of personal data and why, and being able to produce those records if requested. Importantly for arbitrators and smaller law firms, the GDPR's strict record keeping requirements typically do not apply to small and medium-sized enterprises having fewer than 250 employees ("SMEs"), although SME's still need to demonstrate compliance.[42] This means that, as a practical matter, from the outset of an arbitration where personal data covered by the GDPR may be impacted, steps will need to be undertaken to ensure that data protection principles are properly respected during the arbitral process and to be able to demonstrate compliance.

C. One-Stop Shop

With respect to the regulatory structure, the GDPR moves from the decentralized regulatory framework established by the DP Directive - whereby each Member State supervisory authority had broad authority to enforce its national data protection laws - towards a

---

competition law system based primarily on notifications to one based increasingly on self-assessments. *See, e.g.,* Gianfranco Rocca, *Regulation 1/2003: A Modernised Application of EC Competition Rules,* COMPETITION POL. NEWSL. (Eur. Commission, Brussels), Spring 2003, 3, http://ec.europa.eu/competition/publications/cpn/2003_1_3.pdf [https://perma.cc/HV5Y-BD6V] (archived May 30, 2018).

38. *See* GDPR, *supra* note 2, art. 37-39, at 55-56.

39. *Id.*, art. 35, at 53.

40. *See id*, art. 25, at 48

41. *Id.*, art. 5(2), at 36; art. 30, at 57-58.

42. *Id.*, art. 30(5), at 58.

one-stop-shop style system. Under this system, for certain cross-border data processing within the European Union, a lead supervisory authority (the "Lead SA") is given the authority to enforce the GDPR for data custodians having their sole or "main establishment" as defined by the GDPR in that country.[43] The European Union hoped to establish a real one-stop shop whereby one supervisory authority would have exclusive competence,[44] but in the end a compromise was reached whereby issues can typically be raised with the Lead SA or with any "supervisory authority concerned," and a system is established for coordination between the Lead SA and the concerned supervisory authority where necessary.[45] The effect of these rules should be that only one decision is reached on any issue, but who renders it depends on the application of the principles contained in the GDPR, with deference typically given to the Lead SA, if it so requests. When data protection issues affect only one Member State, that country's supervisory authority has authority.[46] Furthermore, when an entity does not have an EU establishment, it must designate in writing a representative in the Union.[47] However, any supervisory authority within the European Union has regulatory authority over that entity without reference to a Lead SA.[48]

As a practical matter, early data mapping will enable parties and their advisors to anticipate what data protection laws will apply, what data protection authority will be the Lead SA, and what other concerned supervisory authorities might be for different aspects of the arbitration and for different data custodians. This will allow the

---

43. *See* GDPR, *supra* note 2, art. 60 at 72; *Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority* 10 (Article 29 Data Protection Working Party, 16/EN WP 244 rev. 01, 2017). [hereinafter "Lead SA Guidelines"]

44. *See* Konrad Lischka & Christian Stocker, *Data Protection: All You Need to Know. About the EU Privacy Debate*, SPIEGEL ONLINE (Jan. 18, 2013, 10:15 AM), http://www.spiegel.de/ international/europe/the-european-union-closes-in-on-data-privacy-legislation-a-877973.html. [https://perma.cc/G7AN-HJGQ] (archived May 30, 2018).

45. "Supervisory authority concerned" is defined as a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority.

See GDPR, *supra* note 2, Art. 4 (22) at 35.

46. *See id.*

47. *See* GDPR, *supra* note 2, art. 27(1), at 48.

48. *See* Lead SA Guidelines, *supra* note 43.

parties and others subject to the GDPR to foresee how those laws and authorities are likely to address the data protection issues that may arise during the arbitration. This information will enable the development of an overall approach to minimize the data protection risks and for managing them during the arbitral process.

D. Global Reach

Due to the inherently trans-border nature of international arbitration, the issue that has received the most attention to date from the international arbitration community to the EU data protection laws are the measures restricting the transfer of personal data outside the European Union. The European Commission has stated that its intent is not to keep EU data in the European Union, but rather to export EU data protection standards by ensuring that the protections move with the data and by encouraging other countries to adopt similar laws so that data moves freely but with an adequate level of protection and data subject rights.[49] Therefore, while the GDPR is obviously not of universal application, the European Union has declared its intent for the GDPR to become the *de facto* international standard for the protection of personal data, through the following general approach:

(1) the use of transfer restrictions to impose GDPR-style obligations whenever EU data is transferred to third countries outside the European Union (referred to as "third countries");
(2) the potential imposition of substantial penalties for violations to ensure compliance;
(3) the extension of the GPDR to the processing of data relating to EU data subjects in third countries where the controller or processor is not based in the European Union but has purposefully targeted the provision of goods and services within the European Union or engaged in monitoring of EU data subjects; and
(4) the insistence on trading partners adopting adequate data protection regimes as a condition of EU trade deals—the European Commission has recently said "the

49. *See* Communication from the Commission, Exchanging and Protecting Data in a Globalized World, COM (2017) 7 final (Jan. 2017). [hereinafter Commission Communication].

> protection of personal data is non-negotiable in trade agreements."[50]

The European Union has been surprisingly successful in this endeavor, with the major holdouts being the United States (except for the Data Privacy Shield), China, and Russia.[51]

Specifically concerning the data transfer restrictions in the GDPR, the European Commission's view is that "the EU regime on international data transfers . . . provides a broad and varied toolkit to enable data flows in different situations while ensuring a high level of protection."[52] The GDPR "toolkit" referred to is discussed in the following Section of this Article in the context of data transfers to third countries during international arbitration. [53] The impact of these restrictions is that, when data transfer is permissible, which may or may not be the case, it is always necessary to ensure that adequate safeguards are in place to protect the data after it is transferred either by operation of law or by agreement.[54]

E. Sanctions

Although the DP Directive allowed Member States to access appropriate fines, the fines imposed were not sufficient to create a culture of compliance. This has changed dramatically under the GDPR and is the most important driver behind the unprecedented focus on GDPR compliance.[55] The potential fines set forth in the GDPR are up to the higher of four percent of a violator's worldwide revenue or EU€20 million for the most serious violations and half of that for less serious infractions.[56] Data subjects also have the right to enforcement before courts and regulatory authorities and to obtain damages, and there is a possibility of criminal sanctions. [57]

A set of guidelines on the assessment of fines under the GDPR has already been issued, which is helpful in understanding how fines will be assessed.[58] During the initial stages of GDPR implementation,

---

50. *Id.*
51. *See* Scott & Cerulus*, supra* note 4.
52. *See* Commission Communication, *supra* note 49, at 6.
53. *See supra* Section III.H.
54. *See* GDPR, *supra* note 2, art. 44 at 60.
55. *See generally*, Scott & Cerulus, *supra* note 4.
56. *See* GDPR, *supra* note 2, art. 83, at 82.
57. *See id.,* arts. 79, 82, at 80-81.
58. *See generally* Guidelines on Fines, *supra* note 10.

large fines are not expected absent serious violations and provided good faith efforts at compliance are undertaken. However, the threat of such fines and other sanctions together with the compliance imperative that has developed around the GDPR means that senior management and directors of companies are now increasingly focused on GDPR compliance. In turn, this means that parties will start to proactively manage the GDPR risk arising from international arbitration. Furthermore, the fact that all Arbitral Data Custodians (including arbitrators) are potentially caught within the GDPR's reach means that everyone has a compliance incentive. The combined impact of these factors means that, when the GDPR is applicable, data protection compliance will become part of the arbitral process. The following Section of this Article addresses the legal framework established by the GDPR and how this applies to international commercial arbitration, followed by a Section addressing the GDPR's potential practical impact on arbitration.

III. GENERAL APPLICATION OF THE GDPR TO INTERNATIONAL ARBITRATION

The GDPR grants data subjects extensive rights with respect their personal data.[59] Many of these rights are difficult to reconcile when applied to international arbitration because of its decision-making function and other characteristics (often including confidentiality). It is important to note that the same concerns arise in the context of court litigation, which is why the GDPR excludes Member State courts and other judicial authorities from supervision by the data protection supervisory authority to preserve their independence. The GDPR suggests instead that the judicial authorities themselves regulate the data used in the judicial capacity.[60] Recital 20 of the GDPR provides as follows:

> While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard

59. *See generally* GDPR, *supra* note 2, art. 12-22, at 39-46.
60. *See id.,* recital 20, at 4.

> the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.[61]

The language refers to "processing of data by courts and other judicial authorities."[62] While the general reference to "judicial authorities" could conceivably cover arbitration, which has a decision-making function similar to a court, this exemption from oversight by the Member State supervisory authority is replaced by enforcement by the Member State court system, which courts do not supervise arbitration. Article 55 of the GDPR provides that "Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity," without any reference to arbitration.[63] Therefore, this general exemption from the supervisory authority does not apply to arbitration nor does it apply to non-EU courts.[64] Furthermore, the exemption of Member State courts from oversight by the supervisory authority does not mean that the GDPR does not apply to the courts, rather it means that that the rules are enforced by the judicial authorities themselves rather than the supervisory authorities.

However, Article 23 of the GDPR does grant the Member States the right to exempt certain activities from the application of many of the specific rights granted to data subjects. This right for Member States to grant exemptions applies "when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard," among other things, "the protection of judicial independence and judicial proceedings" and "the enforcement of civil law claims." This is subject to the proviso that the Member States puts in place adequate safeguards to protect the data subject rights that have been exempted.[65] As mentioned above, Ireland is an example of a Member

61. *Id.*

62. *Id.*

63. *Id*., art. 55, at 67.

64. Burianski & Reindl, *supra* note 15, at 187 (authors reach a similar conclusion under the DP Directive).

65. *See, e.g.*, GDPR, *supra* note 2, art. 23(2), at 47.

State that has relied on Article 23 to exempt certain data subject rights, to the extent that the restrictions are "necessary and proportionate," for the processing of personal data "in contemplation of or for the establishment, exercise or defence of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings whether before a court, statutory tribunal, statutory body or an administrative or out-of-court procedure."[66] The references in the Irish exemption to "out-of-court procedure" covers arbitration.

Application of the Article 23 exemption (including the Irish DP Bill) does not mean the data is excluded from the GDPR, but rather that certain of the data subject rights do not apply. The data subject rights that can be exempted (and which Ireland has exempted) include the rights of the data subject to transparent information (potentially including data privacy notices) (Articles 12, 13 and 14), access to data (Article 15), rectification and erasure (Articles 16 and 17), to restrict further processing (Article 18), data portability (Article 20) and the rights to object and to automated decision making (Articles 21 and 22). [67] These rights are particularly difficult to apply to an arbitration, and can be inconsistent with the arbitrator's decision-making function, including the interactions among arbitrators, and with the institution. The exemption of these rights makes the GDPR more consistent with international arbitration, while at the same time protecting the fundamental goal of the GDPR to protect the personal data of data subjects. It is beyond the scope of this Article to analyze each of the GDPR's provisions in light of the exemptions adopted by the 28 Member States, many of which have yet to be finalized at the time of writing. This Article therefore focuses on the text of the GDPR and the precedents established under the previous DP Directive as they would apply to international commercial arbitration, however, in practice, it will be important to consider Member State laws as well (as well as third country laws).

In addition to the right granted to Member States to exempt certain data and data processing under Article 23, the GDPR itself already contains express exemptions from some provisions for data that is "necessary for the establishment, exercise or defence of legal claims", which, although subject to interpretation with respect to what

66. *See* Irish DP Bill, *supra* note 9, art. 60 (3)(a)(iv), at 46; *see also* Irish DP Bill, *supra* note 9, art. 161, at 136-137.

67. *See, e.g.,* GDPR, *supra* note 2, arts 12-22, at 39-46.

is "necessary", applies to arbitration.[68] The GDPR explains in a recital that, at least in the context of special categories of data, processing should be allowed "where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure" and similar language is included in another recital in the context of data transfers."[69] "Out-of-court procedure" is not defined and the text of the GDPR does not further illuminate what is covered by data processing that is "necessary for the establishment, exercise or defence of legal claims" but on any definition arbitration includes the processing of data "necessary for the establishment, exercise or defence of legal claims" (sometimes referred to herein as the "legal claims exemption").[70]

The legal claims exemption in the GDPR itself applies only to allow the processing of special categories of data, and to exempt data processing from the data subject rights to erasure and to restrict processing (Articles 17 and 18) and the right to object to further processing (Article 21), and as a basis to allow data transfer to third countries. However, Article 23 allows Member State exemption of a much broader category of rights for "the protection of judicial independence and judicial proceedings" and "the enforcement of civil law claims." The other rights covered by Article 23 (especially the rights to data transparency, access to data, and rectification) are difficult to apply to international arbitration and potentially inconsistent with its decision-making function, which led Ireland and potentially other Member States to exempt out-of-court procedures from them. International commercial arbitration has a decision-making function, which is of a judicial character. Reconciling these rights with international arbitration will be challenging, and argues in favor of exempting data subject rights that are inconsistent with the cross-border, consensual, decision-making function of international commercial arbitration, and taking into consideration the fact that it is often confidential.

The remainder of this Section will address each of these questions under the legal framework adopted by the GDPR. The main source of guidance about the application of the data protection rules under the existing system established under the DP Directive is the

68. *See, e.g., id.,* recital 52, at 10.
69. *See id*., recital 111, at 21 (emphasis added).
70. *See, e.g., id*, art 18, at 43.

Article 29 Working Party ("WP29").[71] The Working Party was established under Article 29 of the EU Data Protection Directive, hence its name. It is made up of Member State data protection authorities and relevant EU officials and provide guidance on the application of the DP Directive. The GDPR will replace WP29 with the European Data Protection Board (the "EDPB").[72] The EDPB is empowered to issue guidelines, recommendations, and best practices to encourage consistent application of the GDPR and in the setting of administrative fines.[73] However, the EDPB has yet to be established, therefore, the initial guidelines on the application of the GDPR have also been established by WP29.

WP29 has never addressed the application of the DP Directive or the GDPR to arbitration, although it has addressed the application of the DP Directive to cross border data disclosure for purposes of US litigation.[74] In this context, WP29 has provided a set of guidelines focused primarily on data transfers necessary to comply with US discovery requests (the "Disclosure Guidelines").[75] Given the lack of direct guidance about the application of the GDPR to arbitration, the Disclosure Guidelines and other relevant guidance issued by WP29 under the DP Directive provide useful resources on how these issues may be addressed in the context of international arbitration and will be discussed throughout this Article.[76] However, it remains to be seen how this will actually operate under the GDPR (as opposed to the DP

71. *See* DP Directive, *supra* note 14, art. 29; *Composition & Structure*, EUROPEAN COMMISSION (Oct. 6, 2017), http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=605262 [https://perma.cc/J9N6-R9LN] (archived on Apr. 27, 2018).

72. *See* GDPR, *supra* note 2. art. 70, at 76-78.

73. *Id.*

74. For an excellent overview of EU and national laws concerning data disclosure for litigation, see E-DISCOVERY AND DATA PRIVACY: A PRACTICAL GUIDE (Catrien Noorda & Stefan Hanlose eds., 2011).

75. *See generally Working Document on Pre-trial Discovery for Cross Border Civil Litigation,* (Article 29 Data Protection Working Party, 00339/09/EN WP 158, 2009) [hereinafter Disclosure Guidelines].

76. The Disclosure Guidelines refer to the work of the highly-regarded Sedona Conference, which issued "International Principles on Discovery, Disclosure & Data Protection in Civil Litigation" and a draft protocol for how these issues should be addressed by a court, but nothing similar has been developed for international arbitration. *See generally* SEDONA CONFERENCE WORKING GROUP, THE SEDONA CONFERENCE: INTERNATIONAL PRINCIPLES ON DISCOVERY, DISCLOSURE & DATA PROTECTION IN CIVIL LITIGATION (TRANSITIONAL EDITION), App. D: Cross-Border Data Safeguarding Process + Transfer Protocol (2017) [hereinafter SEDONA PROTOCOL]. The Sedona Protocol for U.S. litigation is set forth in Appendix C of this Article.

Directive) and whether the same principles will be applied to commercial arbitration (as opposed to US litigation) given that arbitration is different from a court proceeding in many ways, including, among other things, that it is often confidential and always consensual. Furthermore, as previously addressed, although it is a regulation, the GDPR will be enacted into Member State laws, which may exempt certain data and data processing during an arbitration from coverage, which means that any consideration of the application of data protection to an arbitration will always begin with applicable law.

A. What does the GDPR apply to in the context of international commercial arbitration?

The 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 Union, whether or not the processing takes place in the Union; and
- 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 relates to the offering of goods or services (whether free or paid for) or the monitoring of behavior which takes place within the European Union.[77]

Appreciating the potential application of the GDPR to arbitration therefore requires understanding:

- What "personal data" is typically reviewed during the context of an international arbitration;
- When and how does the arbitral process constitute the "processing" of personal data;
- Who is covered;
- What obligations apply to covered parties;
- What principles apply to the processing;
- When processing is lawful;
- When can data be transferred to third countries; and
- What this means for international arbitration.[78]

---

77. *See* GDPR, *supra* note 2, art 3, 32-33.

78. GDPR, *supra* note 2, art. 3, at 32-33.

The following discussion will consider each of these questions separately in the context of international commercial arbitration.

B. What "Personal Data" is Typically Reviewed in the Context of an International Arbitration?

With the proliferation of the internet, email, and other forms of digital communication, the data reviewed during the course of an arbitration by the parties, experts, institution, and the arbitrators has become increasingly vast and almost exclusively digital. This data is covered by the GDPR whenever it contains "personal data." The GDPR defines "personal data" as any information relating to an identified or identifiable natural person, who is referred to as the "data subject."[79] An identifiable person is one "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."[80] The European Commission has provided the following examples of personal data:

- a name and surname;
- a home address;
- an email address such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone);
- an Internet Protocol (IP) address;
- a cookie ID;
- the advertising identifier of [a] phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.[81]

The following examples of data are not considered personal data:

---

79. *See id.,* Art 4(1), at 33

80. *Id.*

81. *See What is Personal Data?*, EUROPEAN COMMISSION https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en [https://perma.cc/CJ52-ZQVB] (archived May 31, 2018).

- a company registration number
- an email address such as info@company.com;
- anonymized data.[82]

These examples demonstrate that it is irrelevant to the application of the GDPR that covered personal information is contained in a business-related document (such as work emails, lab notebooks, agreements, construction logs, *etc*.) provided that an individual is identified or identifiable, as exemplified by the Commission's express inclusion of an individual's business email address as one of the listed items constituting personal data. [83]

This means that all business-related information exchanged during a typical arbitration containing information by which an individual is, or could be, identified is "personal data" as defined by the GDPR. This includes whether that information is contained in a single document or any combination of documents.[84] Needless to say, this covers much of the data exchanged during a typical international arbitration. While the evidence submitted and exchanged is typically thought of as being the source of potential data protection concerns, the memorials, witness statements, expert reports, and the award itself are also likely to identify individuals. Therefore, they are also likely to contain personal data covered by the GDPR. Any material of any nature containing personal data covered by the GDPR will be referred to herein as "Personal Arbitral Data."

C. When and How Does the Arbitral Process Constitute the "Processing" of Personal Data?

The GDPR covers all "processing" of Personal Arbitral Data and defines "processing" broadly to include the "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction,

82. *Id.*

83. *See id.*

84. *See* GDPR, *supra* note 2, recital 26, at 5. The GDPR applies to all data by which an individual is identifiable and in determining whether a natural person is identifiable, "account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly." *Id*.

erasure or destruction of personal data."[85] The GDPR further clarifies that its application is "technologically neutral" and does not depend on the techniques used to process the data and that it applies to the processing of personal data by automated means, as well as to manual processing.[86] The European Commission has also provided a list of examples of what it considers to constitute processing:

- staff management and payroll administration;
- access to/consultation of a contacts database containing personal data;
- sending promotional emails;
- shredding documents containing personal data;
- posting/putting a photo of a person on a website;
- storing IP addresses or MAC addresses;
- video recording ("CCTV").[87]

Under such an expansive definition, virtually any activity undertaken during an arbitration relating to documents including Personal Arbitral Data is likely to be considered processing covered by the GDPR, even if it is just shredding documents or taking notes including the names of individuals. During the course of a typical complex international arbitration, the following activities, among others, relating to documents containing Personal Arbitral Data would likely be considered processing covered by the GDPR:

- Document retention;
- Document review;
- Document transfer to a third party engaged to assist during the process, including external providers of electronic data review services, external counsel, or an independent expert engaged by a party;
- Disclosure of materials during the arbitral process to the other party, their counsel or expert, the arbitral

85. *See* GDPR, *supra* note 2, art. 4(2), at 33. The definition requires "the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation." *Id.*, at 3. Given the way that documents are filed in international arbitrations, this exclusion is unlikely to apply.

86. *Id.*, recital 15, at 3.

87. *See What Constitutes Data Processing?*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en [https://perma.cc/Q85B-NJ33] (archived Mar. 19, 2018).

institution or the tribunal (*e.g.* document disclosure, submitted evidence, witness statements, expert reports, memorials);
- Tribunal-ordered disclosure of materials;
- Preparation, exchange and issuance of an award; or
- Document destruction.

The Disclosure Guidelines issued by WP29 under the DP Directive clarify that in the context of data disclosure for US litigation, "there are different stages during the litigation process," including "retention, disclosure, onward transferring, and secondary processing. [88] The use of personal data at each of these stages will amount to processing requiring an appropriate legal basis on which to base the processing."[89] This means that where the GDPR applies to an Arbitral Data Custodian, compliance obligations apply from the time that it is decided to review or retain potential Personal Arbitral Data for later use in an arbitration until the documents containing Personal Arbitral Data are finally destroyed, and every step in between. Thus, it behooves anyone involved in an arbitration where the GDPR is potentially implicated to understand what potential obligations may apply to them.

D. Who is Covered?

Entities that are established in the European Union are covered by the GDPR with respect to all data processed in the context of their activities.[90] This means that Arbitral Data Custodians established in the European Union must comply with the GDPR with respect to all the Personal Arbitral Data they process in the context of those activities. [91] For entities established in the European Union, this includes all processing of personal data wherever it is processed and regardless of whether it relates to EU data subjects.

---

88. Disclosure Guidelines, *supra* note 75, at 7.

89. *See id.*

90. *See* GDPR, *supra* note 2, art. 3(1), at 32.

91. Special rules apply to international organisation institutions, which may include, for example, the Permanent Court of Arbitration and the International Court of Justice. Entities established under international law or by an agreement between countries are treated as though they are outside the European Union such that transfer to them is prohibited absent adequate safeguards. *See* GDPR, *supra* note 2, art 4(26) at 35 (defining international organisations), art. 46 (1) at 62 (addressing transfers to international organisations).

Unlike the DP Directive, the GDPR also applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the European Union where the processing relates to the offering of goods or services (whether free or paid for) or the monitoring of behavior which takes place within the European Union.[92] Entities falling within this category are required to designate in writing a representative in the Union unless the processing is "occasional, does not include, on a large scale, processing of special categories of data [. . .], and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing."[93] This does not mean that anyone who acquires personal data of an EU data subject anywhere in the world in the context of passively offering a good or service within the European Union is governed by the GDPR. Rather it must be shown that the entity intended to offer goods or services to "data subjects in one or more Member States in the Union."[94] The "mere accessibility" of a website or an email address from the European Union is:

> insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.[95]

It is unclear whether this provision applies solely to the processing of EU data in the context of targeted sales of goods and services directly to EU data subjects, which does not include legal entities, or also to the processing of EU data where the processing "relates" to a targeted sale of goods or services to an EU business. The language of the recitals would seem to require that the sales must be targeted to EU data subjects, rather than EU businesses, but this is not clear from the text of the regulation itself and it remains to be seen how this will be interpreted.[96] This distinction could impact the extent

92. GDPR, *supra* note 2, art. 3, at 33.

93. *Id*., art. 27(1)-(2), at 48.

94. *Id*., recital 23, at 5.

95. *Id.*

96. The language of the recitals to the GDPR support the view that it was only intended to cover sales to, and monitoring of, EU consumers. *See id.* Furthermore, Article 3 states that "this Regulation applies to the processing of personal data of data subjects who are in the

to which the GDPR applies directly to parties, counsel, experts, arbitral institutions, and arbitrators, that are not established in the European Union but that make targeted efforts to encourage EU parties to use their services, for example by translating their rules into EU languages, making EU road shows, visiting potential EU parties, posting information about EU-specific capabilities, sponsoring EU conferences, actively having their names included for consideration as arbitrators by EU institutions, or other similar activities, but do not target EU data subjects as such. Applying the narrower construction, these parties would not be covered by the GDPR, but it remains to be seen how this language will be applied in practice to entities or individuals that target EU businesses as a result of which personal data of EU data subjects is processed (including in the context of international arbitration).

E. What Obligations Apply?

Whenever Personal Arbitral Data is processed by an Arbitral Data Custodian falling within the reach of the GDPR, the mandatory rules of the GDPR apply.[97] This means that if a party has undertaken the analysis set forth above and has decided that in the context of the arbitration, it will be processing Personal Arbitral Data in a manner covered by the GDPR, the next question is what rules apply to the processing of that data. The discussion in this sub-Section focuses on the nature of the applicable legal framework, the practical impact of which is addressed in the next Section of this Article.[98]

1. Controllers Versus Processors

The primary obligation for compliance with the GDPR rests on the controller of the Personal Arbitral Data, which is defined by the GDPR as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines 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 behavior as far as their behavior takes place within the Union.

See id, art. 3, at 32-33.

97. *See* GDPR, *supra* note 2, arts. 1-3, at 32-33.

98. *See supra* Part IV.

purposes and means of the processing of personal data."[99] WP29 has clarified that "the *first and foremost role of the concept of controller* is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise the rights in practice. In other words: to *allocate responsibility.* [100] This means that "it is most important to ensure that the responsibility for data processing is *clearly defined* and can be *applied effectively*." [101]

A data controller can also delegate the processing of the data under its control to a data "processor" which is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[102] Under the GDPR, data controllers can only engage data processors who commit to complying with its terms in an enforceable agreement in the manner established in the GDPR.[103] These agreements must "set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller," and shall "stipulate, in particular, that the processor processes the personal data only on documented instructions from the controller."[104]

Both the data controller and the data processor are liable for compliance with the GDPR, but the data processor's liability is more limited because it is acting at the behest of the data controller. Given the complexity of modern data processing arrangements, the GDPR also provides for joint controllers of data when more than one entity jointly determines the purpose and means by which the data is to be processed.[105] In cases of joint control, the GDPR requires the joint controllers to enter into a transparent arrangement allocating the compliance obligations and to inform the data subject thereof.[106] Furthermore, data subjects have an independent right of action against each joint controller. [107]

---

99. GDPR, *supra* note 2, art. 4(7), at 33.

100. *Opinion 1/2010 on the Concepts of "Controller" and "Processor"*, at 4 (Article 29 Data Protection Working Party, 00264/10/EN WP 169, 2010) (emphasis in original) [hereinafter Controller Opinion].

101. *Id.* at 7.

102. GDPR, *supra* note 2, art. 4(8), at 33.

103. *See id*., art. 28, at 49.

104. *Id*., art. 28(3), at 49.

105. *See id.,* art. 26(1), at 48.

106. *See id.*, art. 26(1), at 48.

107. *See id*., art 26(3), at 48.

Considering the stringent obligations imposed by the GDPR on data controllers, there may be a tendency towards increased use of data processing agreements. However, this will only be possible when the nature of the activity supports its characterization as "processing" and where the data controller is willing to accept the increased risk created by taking responsibility for the actions of the data processor. Both the GDPR and relevant case law make clear that even if a data processing agreement complying with the terms of the GDPR is in place, the facts could outweigh that agreement, particularly where the facts support a finding that the data processor determined the purpose for all or part of the processing.[108]

2. General Application to International Arbitration

As set forth above, the GDPR establishes that the controller of the Personal Arbitral Data exchanged during an arbitration is the entity or individual that either alone or with others has the ability to "determine" the "purpose and means" of the processing of Personal Arbitral Data. [109] When applying these concepts, it is important to recall that it is the ability to determine the purpose and means of the processing itself that is determinative.[110] The question is who decides why and how the Personal Arbitral Data is processed in order to undertake its role in the arbitral process, whether it be as a party, a data analyst or lawyer doing an electronic data review to retrieve relevant evidence, counsel preparing a memorial, an independent expert writing a report, a tribunal preparing the award, or an arbitral institution reviewing the award. WP29 has explained that the capacity to "determine" the ways and means of data processing:

> would usually stem from an analysis of the *factual* elements or circumstances of the case: one should look at the specific processing operations in question and understand who determines them, by replying in a first stage to the questions 'why is this processing taking place? Who initiated it?' Being a controller is primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its own purposes.[111]

108. Controller Opinion, *supra* note 100 at 11.
109. GDPR, *supra* note 2, art. 4(7)
110. *See id.*
111. *See* Controller Opinion, *supra* note 100, at 8 (emphasis in original).

Further, "the concept of controller is a *functional* concept, intended to *allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis*."[112]

Absent data processing agreements, for purposes of the GDPR, as discussed in detail in the following Section of this Article,[113] all Arbitral Data Custodians are likely to be considered data controllers both because such control is inherent in their function as counsel, expert, arbitral institution, or arbitrator, and because, as a matter of fact, they "determine" the "purpose and means" by which the Personal Arbitral Data is processed in order to perform that function. Arbitral Data Custodians may be able to alter this designation by entering into data processing agreements in certain contexts, but avoiding controller status will be difficult to achieve given the nature of the arbitral process (except for certain data analysts and potentially lawyers performing that function). This means that in arbitrations covered by the GDPR there likely will be a number of different data controllers each with overlapping obligations (for example to provide data privacy notices) and individual legal liability for each controller for failure to comply with these duties.[114] For arbitration to be efficient, these overlapping rights and duties will need to be allocated amongst the party that first collected the data during its business operations or from employees, typically a party to the dispute (referred to as the "Initial Data Controller"), and the secondary data controllers in a data protection protocol or other legal instrument (such as is foreseen by the GDPR for joint controllers).

F. Principles Applicable to Data Processing

The GDPR requires the data controller to "implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation."[115] These measures should take into account "the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons."[116] This extent to which this risk-based approach may

112. *Id.* at 9 (emphasis in original).
113. *See supra* Section IV.C.1.
114. GDPR, *supra* note 2, art. 83, at 82.
115. *Id.*, art. 24 (1), at 47.
116. *Id.*

be applied to limit the types of measures that must be employed remains unclear. The text would indicate that the measures adopted should be proportionate to the risk, however, WP29 has clarified that the data subject rights must always be adequately protected regardless of the degree of the risk however, the controller's accountability obligation may vary – "for example where processing is small scale, simple and low risk."[117] In other words, according to WP29, it seems that the data protection measures must always be adequate to protect the data subjects rights, but the means of documenting compliance can be more limited depending on the risk.[118] It remains to be seen how this will be applied in practice under the GDPR.

The GDPR establishes the following principles applicable to the processing of personal data covered by its terms:

> (a) [P]rocessed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
> (b) [C]ollected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes (so-called "secondary processing");
> (c) [A]dequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed ("data minimization");
> (d) Accurate and, where necessary, kept up to date;
> (e) Kept in a form that permits identification of data subjects for no longer than necessary given the purposes for which the personal data is processed (which limits data retention);
> (f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.[119]

117. *Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks 3* (Article 29 Data Protection Working Party, 14//EN 218 WP 169, 2014).

118. *Id.*

119. *See* GDPR, *supra* note 2, art. 5(1), at 35-36.

Data controllers are "responsible for, and must be able to demonstrate compliance with," these principles.[120] The GDPR contains no exemptions from these basic principles.[121]

The GDPR establishes stricter rules for the processing of "special categories" of personal data (previously referred to in the DP Directive as "sensitive data"). Special categories of data are those that reveal "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."[122] The processing of this data is expressly prohibited except in certain limited circumstances, including where "processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity."[123] Hence "special categories" of data may be processed during an arbitration when "necessary for the establishment, exercise or defense of the claims." The meaning of necessary in this context is not defined in the GDPR nor is guidance given about how it might be applied.

G. When Processing Personal Arbitral Data Is Lawful

Under the approach adopted by the GDPR, all processing of personal data is prohibited unless it is expressly allowed. [124] Although counterintuitive in a digital world, this is the way the GDPR and the DP Directive operate. Article 6 of the GDPR provides that:

> Processing shall be lawful only if and to the extent that at least one of the following applies:
>
> (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
>
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject;

120. *Id.*, art. 5(2), at 36.
121. *See id.*, art. 23 at 46-47.
122. *Id.* art. 9(1), at 38.
123. *Id.* art. 9(2)(f), at 38.
124. *Id.*, art. 24, at 47.

> (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
>
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[125]

The Disclosure Guidelines expressly address the lawfulness of data processing for disclosure purposes, among other things. Although not directly on point because they address discovery for US civil litigation, rather than international arbitration, and they were issued under the DP Directive rather than the GDPR, they provide useful guidance on this and other issues.[126] The Disclosure Guidelines recognized the tension between compliance with EU data protection laws and disclosure obligations and further that parties "have a legitimate interest in accessing information that is necessary to make or defend a claim, but this must be balanced with the rights of the individual whose personal data is being sought."[127] With respect to when data may be lawfully processed for purposes of disclosure, the Disclosure Guidelines considered that data processing for disclosure purposes is potentially lawful only when one of three of the exceptions listed in Article 6 of the GDPR is applicable (which were also lawful bases under the DP Directive), namely, the data subject gives consent, the disclosure is necessary for compliance with a legal obligation, or the disclosure is necessary for the legitimate interests of the controller.[128] Note that the legal claims exemption does not constitute a lawful basis for processing under either the DP Directive

125. *Id.,* art. 6(1), at 36.

126. *See generally* Disclosure Guidelines, *supra* note 75.

127. *Id.* at 2.

128. *See* GDPR, *supra* note 2, arts. 6(a), (d) and (f), at 36-37. Although arbitration is creature of contract, the arbitration agreement is not typically with the data subject whose personal data is included in the Personal Arbitral Data provided by a party to the arbitration. Rather, the agreement to arbitrate is usually between the data subject's employer or business partner, etc., and a third party. Provisions (b) and (c) allowing processing in the context of contractual arrangement would therefore usually not apply to data processing in an arbitration. *See* GDPR, *supra* note 2, arts. 6 (b)-(c), at 36.

or the GDPR, although it has been added as a lawful basis for transfer under the GDPR (and query how one could transfer without processing).[129]

1. Consent

The Disclosure Guidelines recognized that consent is a lawful basis for data processing under the DP Directive, but took the view that consent alone should not be considered lawful grounds for transferring EU data to the United States for the purposes of litigation unless the controller can produce:

> [C]lear evidence of the data subject's consent in any particular case and may [also] be required to demonstrate that the data subject was informed as required. If the personal data sought is that of a third party, for example, a customer, it is at present unlikely that the controller would be able to demonstrate that the subject was properly informed and received notification of the processing.

Similarly, valid consent means that the data subject must have a real opportunity to withhold his consent without suffering any penalty, or to withdraw it subsequently if s/he changes his or her mind. This can be particularly relevant if it is employee's consent that is being sought. As the Article 29 Working Party states in its paper on the interpretation of Article 26(1) of the DP Directive: "relying on consent may . . . prove to be a 'false good solution', simple at first glance but in reality complex and cumbersome."[130] The Working Party does recognize that there may be situations where the individual is aware of, or even involved in the litigation process and his or her consent may properly be relied upon as a ground for processing.[131]

This would seem to mean that individuals who are closely involved in the arbitration (for example senior executives engaged in the underlying transaction that is the subject of the arbitration and potentially other witnesses) sometimes may be able to give valid consent. However, this would be a factual determination and highly fact specific. Furthermore, the GDPR clarifies that consent must be as

---

129. *See* GDPR, *supra* note 2, art. 49 (1) (e), at 64-65.

130. *See Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (Article 29 Data Protection Working Party, 2093/05/EN WP 114, 2005) [hereinafter Article 26 Interpretation].

131. *See supra* Section III (introduction) discussing the Disclosure Guidelines, *supra* note 75, at 8.

easy to withdraw as to give,[132] which limits its usefulness as a basis for data processing in international arbitration because once the documents have been relied upon they cannot simply be withdrawn.

2. Necessary for Compliance with Legal Obligation

The Disclosure Guidelines clarified, which is now enshrined in the GDPR, that the need to comply with a legal obligation only legalizes data processing where the legal obligation is created under Member State law, not third country law. Further, this only applies where the data transfer is required to comply with such a legal obligation, which would not include a tribunal order to produce documents.[133] This means that this ground for lawful processing typically would not apply to international arbitration except perhaps in rare circumstances.

3. Legitimate Interest

The Disclosure Guidelines take the view that the legitimate interests[134] of the controller or a third party could support the lawfulness of data processing for disclosure purposes, if this interest is not overridden by the interests or fundamental rights and freedoms of the data subject. WP29 has explained as follows:

> Clearly the interests of justice would be served by not unnecessarily limiting the ability of an organization to act to promote or defend a legal right. The aim of the discovery process is the preservation and production of information that is potentially relevant to the litigation. The aim is to provide each party with access to such relevant information as is necessary to support its claim or defence, with the goal of providing for fairness in the proceedings and reaching a just outcome.

---

132. *See* GDPR, *supra* note 2, art. 7(3), at 37.

133. *See* Disclosure Guidelines, *supra* note 75, at 9.

134. GDPR, *supra* note 2, recital 47, at 12 (stating that a "legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.")

> Against these aims have to be weighed the rights and freedoms of the data subject who has no direct involvement in the litigation process and whose involvement is by virtue of the fact that his personal data is held by one of the litigating parties and is deemed relevant to the issues in hand, *e.g.* employees and customers.
>
> This balance of interest test should take into account issues of proportionality, the relevance of the personal data to the litigation and the consequences for the data subject. Adequate safeguards would also have to be put in place and in particular, there must be recognition for the rights of the data subject to object [to the processing . . .] and, in the absence of national legislation providing otherwise, there are compelling legitimate grounds relating to the data subject's particular situation.
>
> As a first step controllers should restrict disclosure if possible to anonymised or at least pseudonymised data. After filtering ("culling") the irrelevant data – possibly by a trusted third party in the European Union – a much more limited set of personal data may be disclosed as a second step.[135]

The principles established in the Disclosure Guidelines for the lawfulness of data processing for litigation discovery are likely be applied to the lawfulness of data processing for arbitration, but taking into account the consensual nature of arbitration and any confidentiality provisions. These principles established by the Disclosure Guideline support the lawfulness of the processing under the legitimate interest standard provided the data being processed during the arbitration is proportional, relevant, and adequate safeguards are put in place to protect the data subject, including culling data before disclosure and where possible anonymizing or pseudonymizing the data. This argues in favor of limiting the amount of data being processed in order to comply with this guidance.

H. When Personal Arbitral Data Can Be Lawfully Transferred Outside the European Union

The GDPR prohibits transfers of personal data to third countries unless this is expressly allowed by the GDPR. The GDPR establishes rules allowing third country data transfers where:

---

135. *See* Disclosure Guidelines*, supra* note 75, at 9-10.

(1) a tribunal has ordered the disclosure of documents under a treaty,
(2) the country has been deemed to provide adequate protections (including the US privacy shield),
(3) the controller or processor has put in place "appropriate safeguards" to protect the data in one of the means expressly prescribed by the GDPR, or
(4) one of a list of specified derogations apply, including where the processing is "necessary for the establishment, exercise or defence of legal claims." [136]

Furthermore, regardless of the means employed by a party to transfer personal data out of the European Union, the recipient of the data must be required by law or by agreement to apply adequate protections, including the main principles of the GDPR, to the data after it is transferred.[137]

1. Transfers Ordered by Tribunals

With respect to transfers of data ordered by a tribunal, the GDPR provides that:

> Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner *if based on an international agreement, such as a mutual legal assistance treaty*, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer." [138]

The GDPR is therefore clear that if the data transfer order is not based on an international treaty, this provision does not apply. Given the lack of an applicable legal instrument for data transfers in support of arbitration, this provision will not apply in international arbitrations except in rare circumstances. Data transfer to third countries in support of arbitration will therefore need to fall under one of the other categories of data transfers generally permitted.

---

136. *See* GDPR, *supra* note 2, arts. 45-49, at 61-65
137. *See id.*, art. 44 at 60.
138. *Id.*, art. 48, at 64 (emphasis added).

2. General Third Country Transfer Restrictions

WP29 has explained that the exceptions allowing data transfers follow a cascade approach. Where there is an adequacy decision allowing data transfers to that country, this will apply. When data is to be transferred to a country without an adequacy decision, one of the expressly listed "adequate safeguards," should be put in place where feasible, rather than reliance on a derogation.[139] The derogations therefore should be relied upon only when there is no adequacy decision and adequate safeguards are not feasible.[140] Lastly, only when the express derogations are not applicable, may a party rely on its "legitimate interests" as a basis for transfer.

The first question is therefore whether the third country to which data would be transferred has been found to have an adequate level of protection.[141] An adequacy decision is when the European Union has decided based on established set of criteria that a country's data protection laws are adequate, which allows data to be transferred without any further authorization or notice because adequate protections apply as a matter of law.[142] Applying this standard, the European Union has issued favorable adequacy decisions allowing free data transfers to a number of countries, including to the United States where the entity has signed up to the Privacy Shield (only) and Canada for commercial organizations (only).[143]

Where data is to be transferred to a country without an adequacy decision, including to the United States unless the recipient has signed up to the Privacy Shield, the GDPR allows third country data transfers where "appropriate safeguards"[144] are put in place by the controller or processer to ensure protection of the data through a series of mechanisms, including:

(1) Binding corporate rules, which establish a binding code of conduct for a group of companies or a group of

139. *See* Article 26 Interpretation, *supra* note 130, at 4-10.

140. *Id.*

141. *See* GDPR, s*upra* note 2, art. 45, at 61.

142. *See id*., art. 45 (3) at 61.

143. *See* GDPR, *supra* note 2, art. 45(1), at 61. The European Union considers that the data protection laws of Andorra, Argentina, Canada (commercial organizations only), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, United States (privacy shield only), and Uruguay are adequate. Japan and South Korea are in the process of adequacy discussions as part of their trade deals with the European Union. *See* Commission Communication, *supra* note 49 at 7.

144. *See* GDPR, *supra* note 2, art. 46(1), at 62.

> companies engaged in a joint economic activity that they will comply with an approved set of data protection rules;[145]
>
> (2) Verbatim adoption of standard contractual clauses that have previously been approved by the European Commission;[146]
>
> (3) Binding commitments to adhere to approved codes of conduct or certifications; or
>
> (4) *Ad hoc* contractual arrangements between the EU transferor and the third country recipient of the data that have been approved by a concerned supervisory authority.[147]

The GDPR then establishes the approval methods and other procedural safeguards applicable to each mechanism, which vary.[148] To date under the DP Directive, these approval mechanisms have been time consuming and expensive, although the European Commission has issued assurances that this will improve under the GDPR.[149]

WP29 recognized that in the context of litigation, adequate safeguards may not be feasible, but safeguards are the preferred route when they are. Where putting adequate safeguards in place is not feasible, the GDPR contains a list of seven derogations where data can permissibly be transferred without an adequacy decision or appropriate safeguards, namely:

> (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfer for the data subject due to the absence of an adequacy decision and appropriate safeguards;
>
> (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
>
> (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

---

145. *See id.*, arts. 46-47, at 62-63.
146. *See id*., arts. 46, 93(2), at 69, 95.
147. *See id*., arts. 46, 93(2), at 69, 86.
148. *See id*., arts. 45-49, at 61-65.
149. *See* 2018 Communication, *supra* note 26.

> (d) the transfer is necessary for important reasons of public interest;
>
> (e) *the transfer is necessary for the establishment, exercise or* defence *of legal claims;*
>
> (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
>
> (g) the transfer is made from a [public] register. [150]
>
> . . .

The GDPR therefore contains a derogation provision that expressly allows data transfers to third countries where the transfer is "necessary for the establishment, exercise or defence of legal claims."[151] Further, as discussed above,[152] although the language is somewhat opaque, Recital 111 of the GDPR expressly states that the reference to a legal claim applies "regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies."[153] This will therefore form a possible basis for third country data transfers of data "necessary for the establishment, exercise or defence of legal claims" in international arbitrations.

Furthermore, where a transfer "could not" be based either on an adequacy decision, an adequate safeguard, or one of the specific seven derogations listed above, the GDPR also allows:

> transfer to a third country or an international organisation . . . only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights of the data subject and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall [also] . . . inform the data subject of the transfer and of the compelling legitimate interests pursued.[154]

---

150. *See* GDPR, *supra* note 2, art. 49(1), at 64 (emphasis added).
151. *Id.*, art. 49(1)(e), at 64.
152. *See infra* Section III (introduction).
153. *See* GDPR, *supra* note 2, recital 111, at 21.
154. *Id.*, art. 49, at 71.

However, because the GDPR expressly allows transfers that are necessary for the establishment, exercise, or defense of a legal claim, which would apply to certain aspects of an arbitration, the general derogation for legitimate interests would usually not be applicable to data transfers in arbitration (although it could be relied upon for data not covered by the legal claims exemption). Furthermore, because the legitimate interest derogation for third country transfers requires notification of the transfer to a supervisory authority and to the data subject and the derogation for legal claims does not, Arbitral Data Custodians are more likely to rely upon the legal claims derogation where applicable.

The GDPR provides generally that all third country transfer provisions "shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."[155] WP29 has reiterated that even when a derogation is relied on for transfer, safeguards must be put in place to ensure that the processing is carried out with an adequate level of protection and the data subject rights are not circumscribed.[156] Further, advance notice of the transfer should be given to the data subject at least when the transfer is undertaken pursuant to the legitimate interest standard.[157]

As discussed below, in the context of an arbitration, these safeguards would be based on party agreement where possible, but also would need to be agreed to by the tribunal and the institution with respect to the Personal Arbitral Data they process or transfer cross border.[158] This is likely to be done by agreement of the parties and set forth in a data protection protocol that is implemented through a stipulation or tribunal order signed by everyone receiving Personal Arbitral Data during the course of the arbitration. Among other things, the data protection protocol should set forth the basic standards applied to all parties in the process and establish responsibilities for compliance among Initial Data Controllers and secondary controllers.

---

155. *Id*., art. 44, at 60.

156. *See* Article 26 Interpretation, *supra* note 130, at 9; GDPR, *supra* note 2, art. 44, at 60.

157. *See* GDPR, *supra* note 2, art. 13(1)(f), at 46; art. 14(1)(f), at 47; art. 49 (1) at 71.

158. *See infra* Section IV.C.

IV. PRACTICAL IMPACT OF THE GDPR ON THE ARBITRAL PROCESS

Multinational companies today have data protection policies and systems in place. However, the possible application of the GDPR's data protection policies to future arbitral disputes was usually not the first consideration when those policies were formulated. Further, the individuals charged with deciding the dispute resolution systems to be employed by the company were rarely focused on how the data protection rules could impact a later arbitration or other legal proceeding. This lack of alignment can lead to unwelcome surprises.

Although the relevant data set reviewed for an international commercial arbitration is typically smaller in international arbitration than it would be in US litigation, in major arbitration cases the amount of data collected and reviewed is significant. This data set is typically collected or assessed voluntarily by the party bringing the claim, before any claim is brought, and is much larger than the data that is used in the arbitration. Where it applies, the GDPR will need to be complied with respect to the processing of all this data.

The issues raised by the document review typically undertaken in a complex international arbitration are not unique, and the principles that have been adopted to deal with these issues when they arise in civil litigation are relevant to international arbitration. However, in the litigation context, these issues have typically arisen mainly in relation to common law litigation, usually in the United States. This is because European civil law systems are typically not document-intensive and do not require significant document disclosure.[159] As others have rightly pointed out, this means that the provisions of the European data protection law are not tailored for the document-intensive nature of today's typical complex international arbitration process and the principles are not always easy to reconcile.[160] Indeed, while the GDPR expressly addresses the legal obligations imposed by Member State law and excludes its application to Member State judicial proceedings, it expressly refers to "out-of-court procedures" only twice, both times in recitals only, and with no explanation of what this covers or what rules would apply. Hence, until the supervisory authorities, EDPB, the Member

159. Burianski & Reindl, *supra* note 15, at 188.

160. *See id.* at 199; KUNER & COOPER, *supra* note 13, at Sections 4.86-4.89, 146-147.

States or the EU provide guidance, the GDPR will be applied to arbitration on an *ad hoc* basis, which creates significant uncertainty about how it will impact arbitral proceedings.

This Section of the Article will consider the potential practical impact of the GDPR on international arbitration. It is divided into three subsections according to the time-line of a potential arbitration. Subsection A addresses the issues that arise before any dispute is raised in putting in place data protection policies that are consistent with international arbitration. Subsection B addresses the data protection implications during the second stage of the arbitral process when the dispute has arisen but before the arbitral tribunal has been appointed. Subsection C addresses how data protection rules may impact the arbitration itself after the tribunal has been appointed, including what data protection rules may apply, the adoption of data protection protocols, and the impact of data protection on disclosure. Appendix A to this Article contains a list of some of the questions that the parties and their counsel may consider asking themselves in planning for the arbitration during stages one and two. Appendix B includes a list of some of the questions that Arbitral Data Custodians could consider during the arbitration. Appendix C includes a sample protocol addressing data protection in the context of US discovery that was developed by the Sedona Conference. Appendix D provides a proposed template of a data protection protocol for arbitrators and the parties to address data protection compliance in international commercial arbitration cases where the GDPR applies (hereinafter "ARBITRAL DATA PROTECTION PROTOCOL"). The issues addressed herein and included in the Appendixes are not intended to be exhaustive.

A. Pre-Dispute Framework

This subsection of the Article addresses the issues that arise before any dispute is raised in putting in place data protection policies that are consistent with international arbitration. Companies subject to the GDPR are currently in the process of constructing and executing a path for compliance with its terms at significant expense, potentially including dispute resolution. From the outset, the individuals tasked with GDPR compliance should work with the in-house and external counsel to consider whether, and if so, how, the GDPR could impact arbitration agreements and existing and future international arbitrations. Where the GDPR is applicable, this includes building

means into the arbitration for ensuring compliance during the arbitral process in a manner that is proportionate to the risk and does not infringe on the due process rights of the parties. [161]

Companies subject to the GDPR that are likely to be engaged in international arbitration should state in their data protection policies that personal data may be processed during future dispute resolution procedures and providing the legal basis for that processing. If it is possible that the personal data will be transferred outside the European Union as part of the dispute resolution process, this should be included in the policy. The information must be provided to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.[162] The GDPR states in this context that "the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data." [163]

1. Secondary Processing for Arbitration

Most of the Personal Arbitral Data presented during an arbitration will have originally been collected in the context of an employment or business relationship and its original purpose was to fulfill those functions. Now a dispute has arisen, and the issue is whether that data can be processed in the arbitration. This is often referred to as secondary processing and the rules applicable thereto apply.

The GDPR provides in Article 5 that personal data must be processed "in a transparent manner in relation to the data subject"[164] and must be "collected only for specific, explicit and legitimate purposes and may not be further processed in a manner that is inconsistent with those purposes." Article 6 allows secondary processing for purposes that are "compatible" with the original purpose.[165] In deciding whether the purpose is compatible, the following is to be considered:

161. *See generally* GDPR, *supra* note 2, art. 25 at 55.
162. *Id*., art. Art. 12, at 39.
163. *Id*., recital 39, at 7.
164. *Id*., art 5 (1) and (b), at 35.
165. *Id.*, art. 6(4), at 37.

> (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
>
> (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
>
> (c) the nature of the personal data, in particular whether special categories of personal data are processed . . . or whether personal data related to criminal convictions and offences are processed;
>
> (d) the possible consequences of the intended further processing for data subjects;
>
> (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.[166]

This is a highly case and fact specific analysis. For example, the use of employee and business-related information in an arbitration of a claim in which the data subject's actions are at issue would often be linked to the purpose for which the data was collected, and, depending on the employee's role, expected in the context in which it was collected. In making this determination, although not determinative, it is helpful that the data subject was informed in advance of the possibility that his or her personal data could be used in a later dispute resolution procedure, and preferably have consented.

2. Data Retention for Future Disputes

Data retention is considered "processing" under the GDPR.[167] The GDPR requires controllers to set retention periods at the time of data collection with the goal of minimizing the data being processed.[168] However, retention is an area where it is potentially difficult to reconcile the requirements of the GDPR with those of international arbitration. Concerning data retention for US litigation, WP29 stated in the Disclosure Guidelines issued under the DP Directive that:

> Various issues are raised in relation to retention . . . . It is unlikely that the data subjects would have been informed that their personal data could be the subject of litigation whether in their own country or in another jurisdiction. Similarly given the

166. *Id.*
167. *See* art. 5 (1) (e) at 36; Disclosure Guidelines, *supra* note 75, at 7-8.
168. *See* GDPR *supra* note 2, art. 5 (1) (b), (c) and (e) at 35-36.

> different time limits for bringing claims in different countries, it is not possible to provide for a particular period for retention of data.
>
> Controllers in the European Union have no legal ground to store personal data at random for an unlimited period of time because of the possibility of litigation in the United States however remote this may be. The US rules on civil procedure only require the disclosure of *existing* information. If the controller has a clear policy on records management which provides for short retention periods based on local legal requirements it will not be found at fault with US law. It should be noted that even in the United States there has recently been a tendency to adopt restrictive retention policies to reduce the likelihood of discovery requests.
>
> If on the other hand the personal data is relevant and to be used in a specific or imminent litigation process, it should be retained until the conclusion of the proceedings and any period allowed for an appeal in the particular case. Spoliation of evidence may lead to severe procedural and other sanctions.
>
> There may be a requirement for "litigation hold" or pre-emptive retention of information, including personal data. In effect this is the suspension of the company's retention and destruction policies for documents which may be relevant to the legal claim that has been filed at court or where it is "reasonably anticipated".
>
> There may however be a further difficulty where the information is required for additional pending litigation or where future litigation is reasonably foreseeable. The mere or unsubstantiated possibility that an action may be brought before the U.S. courts is not sufficient.
>
> Although in the US the storage of personal data for litigation hold is not considered to be processing, under Directive 95/46 any retention, preservation, or archiving of data for such purposes would amount to processing. Any such retention of data for purposes of future litigation may only justified under Article 7(c) or 7(f) of Directive 95/46.[169]

This language implies that the need to have access to data for a later arbitration may not be a sufficient basis on its own to retain data longer than is otherwise reasonable. On the other hand, an arbitration can take place long after the disputed facts occurred and the decision-

169. Disclosure Guidelines, *supra* note 75, at 7-8.

making based on those facts may be significantly hindered if contemporaneous data is not available about the factual context in which the dispute arose. Data retention therefore will be an area where it is important for the data protection team to have detailed input from the legal department and external counsel before establishing the retention policies, as balances may have to be struck.

3. Consent to Processing for Future Disputes

When possible, companies likely to be engaged in international arbitrations should consider having data subjects give express "freely given, specific, informed, unambiguous,"[170] consent to the processing of his or her data for the purpose of future disputes. This consent should include a complete, understandable description of the potential data protection risks this could entail. If future disputes could involve the transfer of data to third countries, this should be expressly explained in the data protection policy or agreement along with a description of the potential risks that could be raised. When possible, consent should be obtained before any business, contractual or employment relationship is formed, because this increases the chances that consent will be considered freely given.[171]

As discussed above,[172] the processing of Personal Arbitral Data requires a legal basis, one of which is consent. WP29 has stated that consent is unlikely to be a sufficient basis for large-scale processing of personal data during litigation,[173] and this rationale is likely to be applied to international arbitration. However, depending on the facts of this dispute, WP29 also left the door open that for the key players in a dispute, consent may be effective, especially when they are somehow involved in the proceeding, although this consent can always be withdrawn. Furthermore, even when consent does not on its own provide a sufficient basis under the GDPR for processing or transfer, consent is helpful to have when applying the other principles contained in the GDPR to arbitration.[174]

170. GDPR, *supra* note 2, recital 32, at 6.
171. *See* Disclosure Guidelines, *supra* note 75, at 7-8.
172. *See supra* Section III.G.
173. *See* Disclosure Guidelines, *supra* note 75, at 7-8.
174. *Id.*

4. Contractual Arrangements and Arbitration Agreements

Companies and other entities subject to the GPDR are currently in the process of reviewing their agreements to insure compliance. In undertaking that review, companies should consider revisiting how the GDPR affects their existing dispute resolution provisions. Furthermore, consideration should be given in the future to how the GDPR affects dispute resolution obligations in crafting both the underlying agreements and the arbitration agreement.

Where data needs to be transferred outside the European Union during an international arbitration, (for example. because a counter-party or the arbitral institution is not based in the European Union, the arbitration is seated outside the European Union, or an arbitrator or counsel is based outside the European Union or travels outside the European Union and requires access to documents), the first question to be considered is where the data would be transferred and whether the European Union has made an adequacy finding with respect to that country or whether the transferee has signed up to the Privacy Shield in the United States.[175] If that is not the case, an increasing number of agreements will contain express provisions addressing data protection obligations either in the form of the standard contract clauses already approved by the European Commission or on an *ad hoc* basis approved by a competent supervisory authority. If properly crafted, these can be relied upon to transfer Personal Arbitral Data to the counterparty and potentially others if they agree to comply with them.

With respect to the dispute resolution provisions, the parties to an agreement should undertake a data mapping exercise to consider whether any Personal Arbitral Data covered by relevant data protection regimes, including the GDPR, is likely to be exchanged during the arbitration, and, if so, how this affects the potential dispute resolution options and whether this should be reflected in the arbitration agreement. Although third country transfer should be possible for the reasons outlined above, avoiding the additional time, cost, and restrictions this entails may lead EU companies that will need to exchange Personal Arbitral Data to use GDPR compliance risk as a basis to insist on arbitration being seated in the European Union and subject to the rules of an institution established either in

175. GDPR *supra* note 2, art. 45, at 68.

the European Union or in a third country with an adequacy decision.[176]

Concerning important arbitration centers outside the European Union, Switzerland has an adequacy decision.[177] Although it remains to be seen, after Brexit it is expected that a system will be put in place to allow free data transfers to the United Kingdom, which means that arbitrators based in London and arbitration in the United Kingdom (including the London Court of International Arbitration) are likely to be covered in some way.[178] Notably, no major Asian arbitral institution is based in a country with an adequacy decision, although New Zealand has an adequacy decision in place and Japan and Korea are currently undertaking adequacy discussions with the European Union as part of their trade deals.[179] Many Asian institutions, including the Hong Kong and Singapore International Arbitration Centers, are based in jurisdictions with data protection regimes, but unfortunately those countries have yet to receive an adequacy decision.

In addition to location, parties should consider including provisions in their arbitration clauses expressly addressing data protection at least generally. For example, in an appropriate agreement a clause could be added providing that:

> The Parties agree to apply, and that the tribunal and the institution shall apply, mandatory data protection obligations during the arbitration in a manner that is proportionate to the risk and that adequately protects data subject rights, while preserving the parties' due process rights."

This type of general language may be useful in guiding the parties, counsel, the tribunal and the arbitral institution if data protection issues arise during the course of the arbitration.

B. Commencing the Arbitration

This subsection of the Article addresses the data protection implications during the second stage of the arbitral process when the

176. *See supra* at Section III.H.2.

177. *See supra* note 143.

178. *See* C. Ructici, *Don't Think that Brexit will Save You from the EU Data Protection Rules*, Computer Weekly (March 2016) https://www.computerweekly.com/opinion/Dont-think-that-Brexit-will-save-you-from-the-EU-data-protection-rules [https://perma.cc/P99T-LEGC] (archived May 30, 2018).

179. *See* Commission Communication, *supra* note 49, at 8.

dispute has arisen but before the arbitral tribunal has been appointed. This includes the importance of including the data protection team in planning the arbitration process, data mapping to determine the applicable data protection rules and how they will be enforced, retaining and consulting with external counsel, drafting the arbitration notice, and selecting the arbitrator. Data protection considerations have the potential to impact each of these pre-arbitration steps.

1. Consulting with the Data Protection Compliance Team

The GDPR imposes detailed obligations on companies not only to comply with its provisions but also to be able to demonstrate compliance.[180] This includes documenting the decisions that are taken to ensure GDPR compliance and the rationale for those decisions.[181] SMEs are exempted from some of the more strenuous documentation requirements, and Member States are encouraged to take the needs of SMEs into account when enforcing the GDPR, but SMEs still need to be able to show that reasonable and proportionate compliance efforts were undertaken to comply.[182]

Many companies have or will appoint an independent and autonomous DPO either because they are required to or will did so voluntarily.[183] If a DPO has been appointed, the detailed rules established in the GDPR for consultation with the DPO apply.[184] Thus, if a company has a DPO, that person should be the first stop when arbitration is contemplated. WP29 has issued guidelines on DPOs, which are useful to review in understanding their intended function.[185]

The GDPR also requires the preparation of a data protection impact assessment ("DPIA") for certain types of high risk processing.[186] Absent specific risks, it is unlikely that a DPIA will be required for a typical international commercial arbitration. Nonetheless, this should be considered as part of the documentation of compliance and it is expected that companies may use DPIAs as a

180. *See* GDPR, *supra* note 2, art. 5(2), at 39.
181. *See id*., art. 30, at 57.
182. *See id.*, art. 30 (5), at 58.
183. *See id*., art. 37, at 62.
184. *See id.,* art. 39, at 63.
185. *See generally Guidelines on Data Protection Officers (DPOs)*, (Article 29 Data Protection Working Party, 16/EN WP 243 rev. 01, 2017).
186. *See* GDPR, *supra* note 2, art. 35, at 60.

means of limiting their exposure even when they are not required by the GDPR.

As a practical matter, this means that from the moment that a dispute starts to percolate where personal data covered by the GDPR may be impacted, in-house counsel responsible for the arbitration will be required to work with the GDPR compliance team to undertake steps to ensure that data protection principles are properly taken into consideration when developing the arbitral process and to document what decisions are taken and why. This will be uncharted territory in many companies and differences of view may be exacerbated as the individuals responsible for dispute resolution and data protection and will each consider their needs to be paramount (*i.e.* winning the arbitration versus avoiding potentially serious compliance risk). Given the attention the GDPR is currently receiving, companies should be careful to not to lean too far in that direction in ways that will unnecessarily hamstring current and future arbitrations. The goal should be to comply with the GDPR, while at the same time ensuring that this does not unnecessarily impact the arbitral process.

2. Data Mapping

Early data mapping of where the data relevant to the dispute is located and where it needs to move is essential to data protection compliance. The data protection and legal teams should work together on this process early on when drafting the arbitration agreement and later when a claim arises but before the arbitration is launched. This collaboration permits strategic long-term decisions to be made with respect to how and where data will be reviewed and transferred, which may impact their choices (including counsel, arbitrator, service providers). For example, the teams could employ creative solutions to allow data review from a data room or onsite. However creative solutions often require early thinking and planning, which favors prompt consideration of these issues.

3. Engaging External Counsel

When disputes arise in a relationship that is subject to an arbitration agreement, companies typically consult with external counsel at an early stage in the dispute resolution process. The selection of external counsel is another area where in the future GDPR compliance may become relevant. Exchanging Personal

Arbitral Data with external counsel is covered by the GDPR, which means, for example, that when Personal Arbitral Data is transferred to a third country for purposes of instructing counsel, the transfer must satisfy one of the criteria allowing for transfer discussed above.[187]

Major international law firms will usually have systems in place allowing such transfer (but this is not necessarily the case) and may not be true of smaller or local firms. Moreover, it is easier and less costly for the application of the data protection rules if all the Arbitral Data Custodians have an establishment in the European Union or in a country with an adequacy decision (including the US Privacy Shield) because it will not be necessary to meet the requirements for third country data transfer. Furthermore, parties should be aware that if they voluntarily transfer Personal Arbitral Data out of the European Union, a tribunal may take this into account when deciding whether the data needs to be disclosed to the other side if data protection concerns about the transfer are raised during disclosure. Of course, this decision will depend on the details of each data transfer, but data transfers outside the European Union to countries without either an adequacy decision or adequate safeguards may weigh against prohibiting disclosure of data later in the arbitration due to data protection concerns relating to transfer. In a sense, a party may be considered to have waived the right to object.

4. Notice of Arbitration or Reply to Notice

If a party considers that the GDPR or other applicable data protection laws may have a major impact on the proceedings it may consider including this already in the Arbitration Notice or the Reply. This will put everyone on notice of these concerns early so that they can plan around them from the outset. This will also give credibility to the data protection concerns when they are raised later in the proceedings.

5. Selection of the Arbitrator

In the same way that data protection obligations could play a role in selection of counsel, if a party has serious concerns under the GDPR, it may consider appointing an arbitrator that is established in the European Union or a country with an adequacy decision. The

187. *See infra* Section III.H.2.

recitals to the GDPR state that an establishment implies the effective and real exercise of activity through stable arrangements. The form of the arrangements, for example, whether they are carried out through a branch or a subsidiary, is not relevant. For these purposes, arbitrators from outside the European Union that are associated with an English chambers or other Member State entity, would likely be considered to have an establishment in the European Union for these purposes, particularly if they undertake their services for the arbitration through that chambers. While this would rarely be the deciding factor in an appointment, it might tip the balance between two similarly situated candidates in cases where the transfer of data is expected to be of critical importance.

C. Proceedings

This Section of the Article addresses how the data protection rules contained in the GDPR may impact the arbitration itself after the tribunal has been appointed, including what data protection rules apply, adoption of data protection protocols and the impact of data protection on disclosure. The question of what obligations apply to whom and for which data set is complicated during the arbitral process and is key to understanding the respective responsibilities under the GDPR. This Section of the Article addresses the following issues that may arise during an arbitral proceeding:

- Who controls the Personal Arbitral Data processed during an arbitration?
- What rules apply to the processing of Personal Arbitral Data?
- How will GDPR compliance impact the arbitral process and how can this be managed?

1. Who Controls the Personal Arbitral Data Processed During an Arbitration?

As already briefly discussed above,[188] the obligations contained in the GDPR apply to all Arbitral Data Custodians who are either "controllers" or "processors" of the data. The result of this analysis is that most Arbitral Data Custodians will be considered data controllers subject to the terms of the GDPR, except to the limited extent they

188. *See infra* Section III.E.

may be processors.[189] The parties will typically be the original controllers of the Personal Arbitral Data for the primary purpose for which it was originally collected—doing business, as well as during the course of the arbitration (referred to as the "Initial Data Controllers"). Given the role played by counsel, experts, arbitrators, and the institution in a complex commercial arbitration there are likely to be multiple secondary controllers who engage in secondary processing of the data. The secondary Arbitral Data Custodians will be the controllers or processors only of the Personal Arbitral Data that they actually receive during the course of the arbitration for the secondary purpose of the arbitration itself. This means that the GDPR obligations applicable to them will be limited to the data they process during the course of the arbitration, whereas the Initial Data Controllers will typically control the entire data set.

These overlapping and potentially conflicting commitments of the Arbitral Data Custodians creates complexity and potential confusion in applying the GDPR to the Personal Arbitral Data processed during a complex international commercial arbitration. Interestingly, in the context of data security, WP29 in its Disclosure Guidelines seemed to differentiate the role of the Initial Data Controllers from counsel and other secondary controllers who process the data, but without providing further explanation or guidance as to how these overlapping roles interact. The following discussion will consider the status of each the Arbitral Data Custodians when they process Personal Arbitral Data during an arbitration.

a. Parties

In a typical arbitration, depending on whether one or both of the parties are covered by the GDPR or another data protection law, one or both of the parties will be the Initial Data Controllers of the Personal Arbitral Data under the GPDR. This is because the data will have been originally collected and processed in the context of the party's business operations that are the subject of the arbitration and for which the party controlled the purpose and means of the original processing of the data typically in the context of a business or employee relationship. This means that the initial obligation for compliance with the GDPR in the context of an arbitration typically falls on the parties as the Initial Data Controllers.

189. *Id.*

b. External Counsel

The function of external counsel in an international arbitration is to represent the parties and to decide how to present their case based on the evidence, which typically includes Personal Arbitral Data. Counsel must determine how and why to process that data, which means that they will control the Personal Arbitral Data provided to them by the parties for the purposes of the GDPR. WP29 has taken this view expressly in the context of a barrister processing data in the course of representing a party based on the following reasoning, which could be applied equally to most Arbitral Data Custodians:

> A barrister represents his/her client in court, and in relation to this mission, processes personal data related to the client's case. The legal ground for making use of the necessary information is the client's mandate. However, this mandate is not focused on processing data but on representation in court, for which activity such professions have traditionally their own legal basis. Such professions are therefore to be regarded as independent 'controllers' when processing data in the course of legally representing their clients.[190]

Similarly, WP29 has foreseen that accountants will typically be considered data controllers under the GDPR because of the nature of their duties, however, WP29 has also explained that accountants could also be considered processors when they are performing a specific data processing activity under the direction and control of the client.[191] Following the same logic, legal counsel covered by the GDPR may try to limit their compliance obligations by entering into data processing agreements when they are asked to review large amounts of data in a function akin to that of the data analyst discussed below.[192] However, limiting counsel's obligations under the GDPR requires the law firm and the client to enter into a data processing agreement as set forth in the GDPR, which may be difficult given the nature of the attorney-client relationship and because of client resistance (although at the end it may be a question of cost and risk).

These issues are not easy to resolve, but counsel concerned about additional risk can reduce the amount of data that they review by having the parties conduct the initial data review and scrub the

190. Controller Opinion, *supra* note 100, at 28.
191. *Id.* at 29.
192. *See infra* Section IV.C.1.c.

data internally or by using data analysts. This limits the data being transferred to them, hence reducing their GDPR compliance risk, but at the same time relinquishes counsel's control over the initial data review. This is happening anyway for cost reasons and as data review becomes increasingly sophisticated through the use of artificial intelligence, but data protection concerns may prove to be an additional driver towards the use of specialized data analysis and e-discovery services.

c. Data Analysts

A data analyst or other e-discovery professional typically processes data on behalf of either the party or its counsel.[193] The use of data analysts is increasingly becoming the norm in conducting the initial data review to scrub and cull electronic data before it is provided to counsel.[194] Using a data analyst requires a high degree of trust because the analyst will be responsible for reducing the data set provided to counsel and to the parties to review for the arbitration and potentially provide to opposing counsel.

A data analyst will typically be considered a "data processor" under the GDPR, rather than a controller, when it:

(1) acts under the instruction of the party or the lawyer in undertaking its tasks,
(2) does not decide the purpose of the data processing and,
(3) is retained under a GDPR-compliant data processing agreement.[195]

This is the view adopted by WP29 in the Disclosure Guidelines.[196] However, there may be circumstances where the data analyst works so closely with the law firm or a party that the data analyst would properly be considered a "joint controller" under the GDPR. Furthermore, even if a data analyst is deemed to be a data processor, WP29 has taken the view in the context of the DP Directive:

193. *E-Discovery: Must-Knows, Landmines, and What the Future Holds*, YOUR ABA (Mar. 2017), https://www.americanbar.org/publications/youraba/2017/march-2017/e-discovery-specialists-can-provide-competence—oversight-for-la.html [https://perma.cc/CH78-CYBQ] (archived May 30, 2018).

194. *Id.*

195. *See generally* Disclosure Guidelines, *supra* note 75.

196. *See id.*

> The external service providers will also have to comply with the principles of the [DP] Directive. They shall ensure that the information is collected and processed in accordance with the principles of the Directive and that the information is only processed for the specific purposes for which it was collected. In particular they must abide by strict confidentiality obligations and communicate the information processed only to specific persons. They must also comply with the retention periods by which the data controller is bound. The data controller must also periodically verify compliance by external providers.[197]

These principles are now enshrined in the GDPR.

d. Independent Experts

Parties to complex international commercial arbitrations often engage independent experts to address technical or quantum issues. To prepare their opinions, these experts typically require access to evidence, which will likely include Personal Arbitral Data. WP29 suggested in the context of the DP Directive that an expert in a litigation might act as a data processor.[198] However, one wonders whether the defined limits on data processors would be consistent with the function of an independent expert. Similar to the barrister example given by WP29 that was discussed above,[199] if the expert is processing the data to prepare an independent report, how could counsel or a party tell the independent expert the purpose or manner in which it could process the data to prepare that report while maintaining the expert's independence? While it may be possible to construct such an arrangement, in principle this seems inconsistent with the role of an independent expert.

e. Arbitral Institution

The function of an arbitral institution is to administer arbitrations according to the institution's rules and practices, which often require the parties to include the institution on communications exchanged with the tribunal, including all filings.[200] The institution determines the purpose and means of the processing of the Personal Arbitral Data uncontrolled by either the parties or counsel; like the barrister in the

197. *Id.* at 13.
198. *See* Controller Opinion, *supra* note 100, at 13.
199. *See supra* Section IV.C.1.b.
200. *See, e.g.*, London Court of International Arbitration Rules, art. 3.3 (2014).

example above, the arbitral institution is an independent entity and processes the data it receives for its own purposes. Thus, for purposes of the GDPR, the arbitral institution processes the data contained in those communications and filings, which in turn means that the institution is a controller of the Personal Arbitral Data under the GDPR.

While the arbitral institutions located in the European Union are expected to be prepared to comply with their obligations under the GDPR, this may be less true of arbitral institutions outside the European Union that may have direct or indirect compliance obligations when they process Personal Arbitral Data governed by the GDPR. Although many of those institutions are situated in jurisdictions with data protection regimes, it remains to be seen how this will operate in practice. Furthermore, even EU institutions may struggle with certain of the transfer, data transparency (potentially including data privacy notices), and other restrictions contained in the GDPR, particularly as those obligations apply to case work.

f. Arbitral Tribunal

It is inherent in the arbitral tribunal's function that the arbitrators control the purpose and means by which they process the documents and evidence presented by the parties, which in turn means that they control the data they receive from the parties and the institution during the course of the arbitration. This means that the arbitrators are subject to the GDPR with respect to their activities that constitute the processing of Personal Arbitral Data. Further, the arbitrators will be required to comply with all the GDPR's rules that have not been expressly exempted, including for example, data minimization, data transparency (potentially including data privacy notices), data transfer restrictions, cyber security, and respecting the data subjects others rights. Where not exempted by Member State Law, this raises serious concerns particularly, for example, where the data transparency requirements could be interpreted to require the disclosure of confidential communications among the tribunal members or between arbitrators and the institution. This argues in favor of exempting these rights from their application to international arbitration especially to the extent they impact the arbitral tribunal's decision-making function.

Where consistent with the parties' due process rights, this argues in favor of the tribunal limiting the amount of data presented in order

to limit the data protection risk. For example, the latest version of the IBA Rules make optional whether the tribunal is copied on the disclosure it orders, and data protection risk would strongly argue against the tribunal receiving any additional data. Furthermore, data protection argues in favor of limited document review and defined evidentiary requirements.

g. Summary Re Controllers

For the reasons set forth above, when the GDPR applies to the processing of Personal Arbitral Data in an arbitration, the Arbitral Data Custodians generally will be considered controllers of the personal data they process, except the more limited circumstances in which they meet the requirements to be data processors. However, for each Arbitral Data Custodian, the GDPR applies only to the data that it actually processes. This argues in favor of reasonable restrictions on the amount of data being processed. The impact of these rules on the arbitral process is discussed in more detail in the following Section.

2. What Rules Apply to the Processing of Personal Arbitral Data?

The application of the GDPR and other data protection regimes to international commercial arbitration means that whenever Personal Arbitral Data is processed during an arbitration the following will be legally mandated unless exempted by Member State law (among other things): adequate data security, data minimization, transparent data retention policies, transparent processing information (potentially including data privacy notices), third country transfer restrictions, and data breach notifications.[201] The rights to data portability and to erasure and to restrict processing may also be raised, although these rights do not apply where the legal claims exemption applies.

Respecting these rights requires a coordinated compliance effort in a manner that is proportional to the risk while at the same time ensuring the tribunals' decision-making function and the parties' due process rights are respected. Although not directly on point, the guidance from WP29 in the Disclosure Guidelines is helpful in gaining an understanding of how the corresponding obligations in the GDPR may be applied to the processing of Personal Arbitral Data in the context of international arbitration and is referred to in this

201. GDPR *supra* note 2, arts. 12-22, at 39-46; EU Handbook, *supra* note 14, 105.

discussion where relevant. This will often result in the parties and the tribunal agreeing a data protection protocol addressing these issues, which is discussed below.[202]

a. Cybersecurity

Important efforts are underway to implement cybersecurity for international arbitration. This includes the Debevoise & Plimpton *Protocol to Promote Cybersecurity in International Arbitration* launched in 2017[203] and the ICCA/NY Bar/CPR *Draft Cybersecurity Protocol for International Arbitration*, released for consultation in 2018.[204] While not directly on point with respect to the data security requirements of the GDPR, together with the Sedona Protocol,[205]they will provide a useful starting point for applying a risk-based analysis to cybersecurity, and as a structure for how data protection may be addressed in international arbitration. However, it is important to keep in mind that whenever the GDPR applies to Personal Arbitral Data processed in an arbitration, adequate cyber security is mandatory. The GDPR requires the following measures be taken to secure all data covered by its terms:

> 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
>
> (a) the pseudonymisation and encryption of personal data;
>
> (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

202. ICCA/NY Bar/CPR *Consultation Draft Cybersecurity Protocol for International Arbitration* Art. 13 (2018) [hereinafter ICCA Cybersecurity Protocol] http://www.arbitration-icca.org/media/10/43322709923070/draft_cybersecurity_protocol_final_10_april.pdf [https://perma.cc/K52P-MHJL] (archived May 30, 2018).

203. *See* Debevoise & Plimpton *Protocol to Promote Cybersecurity in International Arbitration* (2017) https://www.debevoise.com/~/media/files/capabilities/cybersecurity/protocol_cybersecurity_intl_arb_july2017.pdf.

204. *See* ICCA Cybersecurity Protocol, *supra* note 202. *See also* the excellent discussion the cybersecurity issues raised by international arbitration in Stephanie Cohen and Mark Morril, *A Call To Cyberarms: The International Arbitrator's Duty To Avoid Digital Intrusion*, 40 FORDHAM INT'L L.J. 981 (2017).

205. *See* SEDONA PROTOCOL, *supra* note 76, Appendix C.

> (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
>
> (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
>
> 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.[206]

Similarly, in the specific context of US litigation under the DP Directive, WP29 has said that the data controller shall take all:

> reasonable technical and organisational precautions to preserve the security of the data to protect it from accidental or unlawful destruction or accidental loss and unauthorized disclosure or access. These measures must be proportionate to the purposes of investigating the issues raised in accordance with the security regulations established in the different Member States. These requirements are to be imposed not just on the data controller but such measures as are appropriate should also be provided by the law firms who are dealing with the litigation together with any litigation support services and all other experts who are involved with the collection or review of the information. This would also include a requirement for sufficient security measures to be placed upon the court service in the relevant jurisdiction as much of the personal data relevant to the case would be held by the courts for the purposes of determining the outcome of the case.[207]

It is interesting to note that this language from the Disclosure Notice seems to suppose that the law firm is not an independent data controller in its own right, which conflicts with other advice from WP29.[208] Given the significant risk of getting this wrong, the safer course is for lawyers to consider themselves to be controllers in their own right, but this language supports the view that it would be appropriate to use a data protection protocol to allocate these roles and responsibilities in much the same way the GDPR does for joint controllers.

---

206. GDPR, *supra* note 2, art. 32, at 51.
207. Disclosure Guidelines, *supra* note 75, at 12.
208. *See* Controller Opinion, *supra* note 100, at 28 (finding barristers to be controllers).

It will be for the parties in the first instance to agree what security measures are required by the GDPR during the arbitration.[209] This process of agreeing reasonable data security measures involves a risk analysis of the types and importance of the Personal Arbitral Data being exchanged, the laws applicable to the transfer and processing of the Personal Arbitral Data, the cybersecurity systems and capabilities of all the Arbitral Data Custodians that will be receiving and processing Personal Arbitral Data, the risks if the data were to be exposed, *etc*.[210] Where parties are not able to agree reasonable and proportionate data protection measures, tribunals will be asked to assist in this process and ultimately may be required to impose such measures where agreement proves allusive.[211]

b. Data Minimization

When the GDPR applies to the Personal Arbitral Data being processed during an arbitration, data minimization is mandatory.[212] This may include data scrubbing for relevant data and to eliminate sensitive data as a first step before the data is even processed for the arbitration, and potentially pseudonymization of the relevant data where feasible. With respect to data minimization, WP29 has explained in the context of US discovery under the DP Directive that:

> There is a duty upon the data controllers involved in litigation to take such steps as are appropriate (in view of the sensitivity of the data in question and of alternative sources of the information) to limit the discovery of personal data to that which is objectively relevant to the issues being litigated. There are various stages to this filtering activity including determining the information that is relevant to the case, then moving on to assessing the extent to which this includes personal data. Once personal data has been identified, the data controller would need to consider whether it is necessary for all of the personal data to be processed, or for example, could it be produced in a more anonymised or redacted form. Where the identity of the individual data subject's is not relevant to the cause of action in the litigation, there is no need to provide such information in the first instance. However, at a later stage it may be required by the court which may give rise to

209. *See, e.g.,* ICCA Cybersecurity Protocol, *supra* note 202, art. 13.
210. *See generally* GDPR, *supra* note 2, recital 4, at 3.
211. *See, e.g.,* ICCA Cybersecurity Protocol, *supra* note 202, art. 13.
212. GDPR, *supra* note 2, recital 39, 7

> another "filtering" process. In most cases it will be sufficient to provide the personal data in a pseudonymised form with individual identifiers other than the data subject's name.
>
> When personal data are needed the "filtering" activity should be carried out locally in the country in which the personal data is found before the personal data that is deemed to be relevant to the litigation is transferred to another jurisdiction outside the EU.[213]

Special category data should also be culled and not processed unless necessary to decide the dispute.[214] Although the GDPR allows the transfer of sensitive data when necessary for the establishment, exercise or defense of a legal claim, only the limited data that is deemed to be necessary for that purpose should be transferred.[215] As discussed below, data minimization will also argue in favour of a careful application of the IBA Rules to limit the amount of data disclosed during the arbitration.[216]

c. Pseudonymized Personal Data

WP29 has made clear in the Disclosure Guidelines that it prefers for data that is going to be processed during a dispute resolution process to be pseudonymized using a coding system especially where it will be transferred to a third county. Pseudomization is when data is coded so that the personal data subject is not identified, but in a manner such that the data can later be decoded. This system allows the data to be matched to the data subject if needed during the arbitral process but at least during the early stages of review, names would not be included. Pseudonymization does not fit well with the arbitral process. Technology, of course, makes pseudonymization possible but at a cost, and it is difficult to see how it would work efficiently and cost-effectively in practice given the highly fact-driven nature of the arbitral process. Parties are expected to resist pseudonymization given the difficulties and cost that will be involved. While not determinative, factors weighing against requiring pseudonymization under a proportionality standard would include that the Personal Arbitral Data exchanged be:

---

213. Disclosure Guidelines, *supra* note 75, 10-11 (quoting *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for S. Dist. of Iowa*, 482 U.S. 522, 546 (1987)).

214. *See id*. at 10.

215. *See id.*

216. *See infra* Section IV.C.3.b.

- Minimized and targeted at the issues in dispute (as would be the case if the IBA Rules discussed below are applied carefully);
- Scrubbed to eliminate any sensitive or nonresponsive data; and
- Originally obtained by the arbitral party with the knowledge and preferably consent of the data subject who was placed on notice of the possibility of processing for dispute resolution at the time of data collection.

d. Data Rectification

The GDPR grants data subjects "the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement."[217] This right does not contain an legal claims exemption and, hence, will apply to international commercial arbitration unless validly exempted by a Member State law. However, WP29 has recognized the tension between this right and the requirements of data discovery in the context of disclosure for US litigation and has said:

> [t]hese rights may only be restricted . . . on a case by case basis for example where it is necessary to protect the rights and freedoms of others. The Working Party is clear that the rights of the *data subject continue to exist during the litigation process* and there is no general waiver of the rights to access or amend.
>
> It should be noted however that this right could give rise to a conflict with the requirements of the litigation process to retain data as at a particular date in time and any changes (whilst only for correction purposes) would have the effect of altering the evidence in the litigation.[218]

As WP29 recognized, this right to rectify personal data that has been submitted as evidence in an international arbitration creates tension.[219] It therefore seems unusual, and problematic, that neither this right, nor the right to data transparency includes an exemption for

217. GDPR, *supra* note 2, art. 16, at 43
218. Disclosure Guidelines, *supra* note 75, at 12 (emphasis added).
219. *Id.*

legal claims, which are exempted from the rights of erasure and to preclude data processing and which raise similar tensions. However, data subjects can be required to include a rationale for the rectification, which would be submitted to the tribunal as a basis for the rectification. This means the tribunal would be aware of the rectification and be able to take it into account in its decision making.

e. Rights to Erasure or "Right to be Forgotten" and to Restrict Processing

The data subject has the right to request erasure of his or her personal data.[220] This right is available when:

(i) processing is no longer necessary for the intended purpose,
(ii) the data subject withdraws his or her consent,
(iii) the data subject objects to the processing and there are no overriding legitimate grounds for the processing,
(iv) the processing is unlawful, or
(v) erasure is necessary for compliance with a legal obligation.[221]

In addition to erasing the data, when a controller has made the personal data public, the controller must take reasonable steps, including technical measures, to inform the controllers processing the data of the data subject's request to erase this personal data.[222] Alternatively, a data subject can also request a restriction on the processing of his or her personal data when:

(i) the data subject contests the accuracy of the data,

(ii) the processing is unlawful and the data subject does not want to exercise the right to erasure,

(iii) the controller no longer needs the data for the purposes of the processing but the data subject needs the data to defend a legal claim, or

(iv) (if) a decision on a complaint lodged by the data subject is pending.[223]

220. *See* GDPR, *supra* note 2, art. 17, at 43; rec. 65, at 12.
221. *See id*.
222. *Id*. art. 18, at 44.
223. *Id*.

Importantly, the rights to erasure, and to data processing restrictions, which would be problematic to apply in the context of international arbitration, contain a legal claims exemption for processing that is "necessary for the establishment, exercise or defence of legal claims. This means that the rights of erasure and to processing restrictions would not be applied to international arbitration where the data is deemed "necessary" to the claims or defences. The question will be what is deemed "necessary," which is not defined by the GDPR and may be influenced by the applicable Member State law, at least until the EDPB takes a view.

f. Data Retention

Data retention is another area where the GDPR is difficult to reconcile with international arbitration. Arbitration is a highly fact driven process and in a complex case both sides will want to review the record and process Personal Arbitral Data for the time period in question. However, at least in the context of US discovery of EU personal data, WP29 has taken the view that unlimited retention of data for the purpose of later disputes, for example, until the statute of limitations expires, may be unlawful.[224] Applying this logic to arbitration implies that the need to have access to data for a later arbitration is unlikely to be a sufficient basis on its own to retain data longer than would otherwise reasonable. However, the Disclosure Guidelines were adopted in the context of general litigation discovery in the United States, which is very different to the more limited data disclosure in international arbitration.[225] Furthermore, the data retained for an international commericial arbitration would be limited to the data related to the circumstances surrounding the agreement containing the specific arbitration clause. When there is a specific agreement containing an arbitration clause, retention of the data relating to that contract may be considered more reasonable than the general litigation risk considered in the Disclosure Guidelines.

As a matter of practice, GDPR compliance is likely to necessitate limiting the data retained to that which is considered to be "necessary" for a future arbitration. Data retention therefore may lead to disputes during the arbitral process as parties not subject to the GDPR may retain more robust data than those applying the GDPR

224. *See* Disclosure Guidelines, *supra* note 75, at 12.

225. *See id.*

and therefore will have more contemporaneous data available to support their claims. On the other hand, companies that retain more data may be required to disclose more data, which the other side may have decided not to retain either for strategic or legal reasons, potentially including data protection risk. This imbalance will need to be addressed and depending on the circumstances may have to be rectified to ensure due process.

g. Data Transparency (Including Data Privacy Notices)

At the time data is collected from a data subject, the data subject must be provided with detailed information about the manner and means by which the data will be processed as described in the GDPR.[226] Similar rights attach when the controller did not collect the data in the first place, which often is the case in international arbitration.[227] For example, the law firm did not originally collect the data that it controls after a party transfers data to it for use in an arbitration. The same is true of the arbitrators. Compliance with the transparency requirements of the GDPR obligates all the controllers of Personal Arbitral Data to ensure that data subjects whose personal data may by disclosed as a part of an arbitration are provided with transparent information complying with Articles 12, 13, and 14 of the GDPR, including, among other things, the purpose and legal basis for the processing, the potential for (or fact of) arbitration, the names and details of any recipient of each data subject's data, how the data subject's data may be used in the arbitration, and whether data transfer outside the European Union is contemplated by the arbitration. In a complex arbitration, if applied literally, this could mean potentially tens of data controllers being required to send multiple data privacy notices to potentially hundreds of individual data subjects named in the evidence. Serious concerns have also been raised about data subjects relying on these rights to request data relating to the confidential tribunal communications, potentially including draft awards.

WP29 has made clear that data subject rights to transparent information about the processing of his or her data, access to that data, and the right to rectify it, continue to apply to data when processed for litigation purposes, which seemingly would also include

226. *See* GDPR, *supra* note 2, art. 13, at 40-41

227. *See id.* art. 14, at 41.

arbitration.[228] With respect to the access and notice requirements, WP29 said that "in the context of pre-trial discovery, [transparency] would require advance, general notice of the possibility of personal data being processed for litigation. Where the personal data is actually processed for litigation purposes, notice should be given of the identity of any recipients, the purposes of the processing, the categories of data concerned and the existence of their rights."[229]

Therefore, any justification for withholding such notice in the arbitration context would seemingly need to be something unique to arbitration, for example, confidentiality. However, the GDPR provides that confidentiality can only be a basis for not providing the requisite data privacy notice when "the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy." This standard will typically not be met by arbitral confidentiality generally, although it may apply to counsel who is subject to legal privilege and to the arbitrator's duty of confidentiality.

The GDPR provides that only one data privacy notice needs to be sent to a data subject. However, it does not explain how this should work in practice when there are multiple controllers all of whom are potentially liable (as in the case of arbitration). WP29 seemed to differentiate between the "controller" who had originally collected the personal data involved in the litigation and others (like the law firm and the courts), but without providing any further guidance. One possibility, which is indirectly supported by the Disclosure Notice, would be for the Arbitral Data Custodians to agree in a data protection protocol that the parties, as the Initial Data Controllers, will provide the transparent information about the processing including any required data privacy notices, and that the other secondary controllers would rely on those notices. Moreover, arbitrators and the institution should be excluded from any duty of transparency as it relates to the internal workings of the tribunal and its decision-making function.

This is consistent with the approach taken to joint controllers in the GDPR and is sensible as the Initial Data Controllers are the only ones who have any relationship with the data subjects. However, this

228. *See* Disclosure Guidelines, *supra* note 75, at 12.
229. *Id.*

would not seem to shield the other secondary controllers from liability, which raises the question as the whether the Initial Data Controller should provide indemnities to the other Arbitral Data Custodians, which could also be included in a data protection protocol. It should also be noted that in cases involving extensive records, requiring data privacy notices for all data subjects named in the evidence is not only a significant burden but may also effectively mean that the arbitration is no longer confidential because so many persons will potentially be required to be informed, which is further complicated in sensitive cases when the provision of notice itself could be problematic. Transparent processing information (including data privacy notices) exemplify the problems created by applying the GDPR to arbitration absent a detailed thought-through set of rules for how this is going to work.

h. Third Country Transfers

The third country transfer restrictions apply to any data transfer outside the EU of Personal Arbitral Data during an arbitration by the Arbitral Data Custodians including the parties, counsel, arbitrators, witnesses, data analysts, or the institution. Furthermore, transfer is very broadly interpreted to include, for example, any downloading of a document or an email while outside the European Union, or carrying a lap top storing documents containing Personal Arbitral Data outside the European Union. Each of these transfers of data outside the European Union requires (1) a legal basis and (2) adequate safeguards.[230] This means that when Arbitral Data Custodians are involved in an arbitration that are not established in the European Union (or a country with an adequacy decision) or who would like to access document from outside the European Union (or a country with an adequacy decision), it will be necessary to agree a framework for exactly how and on what basis Personal Arbitral Data will be transferred (including Memorials, witness statements, evidence, expert reports, *etc*.). The basis for transfer may be different for different Arbitral Data Controllers, but it is necessary to have this established in advance of transfer.

Voluntary data transfers between the parties and their counsel, and between opposing counsel, will often be undertaken without involving the tribunal, however, it may be required to give data

230. *See*, EU Handbook, *supra* note 14, at 133.

subjects and the supervisory authority notice of the transfer depending on the legal basis on which it is made. For transfers of Personal Arbitral Data outside the European Union involving the tribunal or the arbitral institution, it will be necessary to memorialize such transfers in a protocol or other document to be signed by all Arbitral Data Custodians receiving or sending such data outside the European Union. This will likely include the legal basis for the transfer and any restrictions imposed on the processing as a basis for the transfer.

i. Data Breach Notification

The GDPR contains strict notification requirements in the case of a data breach, which are likely to apply to all Arbitral Data Custodians.[231] Data controllers are required to notify the supervisory authorities of "a data breach that is likely to result in a risk for the rights and freedoms of the data subject within 72 hours of discovery of the breach."[232] Data subjects must also be notified of the breach without undue delay if the data breach "presents a high risk for the rights and freedoms of individuals," whereas if the data breach only presents *some* risk for individuals, only the data protection authority will need to be notified and not the individual data subjects.[233] The data breach notification must include the cause and nature of the breach (if known) and recommendations for how the potentially affected individuals can mitigate the risks of the breach. The burden to prove the absence of risk in a data breach rests on the controller.[234]

It will be very important to agree upfront exactly what will trigger a breach notification and the process for how data breach notifications will be given and to whom. The 72-hour time period is for notification to the DPA, which means that a shorter time line may apply if there are intermediate steps, for example, notification by an arbitrator, counsel, expert, or institution of a data breach to the parties, who will then notify the supervisory authority and potentially the data subjects affected.[235] The fines for violating the data breach notification requirements are up to EU€10 million or two percent of

231. *See* GDPR, *supra* note 2, arts. 33-34, at 52.
232. *Id.*
233. *Id.*
234. *Id.*
235. *Id.*

annual global turnover gross revenue, which argues in favour of a rigorous data breach notification policy.[236]

j. Right to Data Portability

When a data subject directly provides a controller with his or her personal data, the data subject must be able to request a copy of the data concerned in a "structured, commonly used and machine-readable format" from the controller, if the data was provided on the grounds of consent or a contractual agreement and is subject to automated processing.[237] This allows the data subject to easily transmit the processed personal data to another controller of his or her choice without hindrance by the controller that collected the data in the first place. In international arbitration, this right would potentially apply only to the Initial Data Controller who originally collected the data and typically would not impact the proceedings. The other Arbitral Data Custodians will typically be not be Initial Data Controllers subject to this obligation.

3. How will GDPR Compliance Impact the Arbitral Process and How Can This be Managed?

a. Data Protection Protocols

Data protection issues should be raised and addressed at the earliest possibility during the arbitral process, typically the procedural conference, if not before.[238] Compliance with the requirements imposed by the GDPR or other data protection regimes may necessitate putting in place a data protection protocol or other agreement at the outset of the arbitration addressing a number of data compliance issues affecting not only the parties, but everyone who processes Personal Arbitral Data during the arbitration.[239] Given the circumstances, this may take the form of a party agreement, a

236. *Id.*, art. 83(4), at 82.

237. *Id.,* art 20, at 45.

238. *See* ICCA Cybersecurity Protocol, *supra* note 202, art. 14, at 16 (addressing cybersecurity only).

239. *Cf. generally* ICCA Cybersecurity Protocol, *supra* note 202 (addressing cybersecurity only); *with* SEDONA PROTOCOL, supra note 76, at Appendix C (addressing discovery for litigation only). The ARBITRAL DATA PROTECTION PROTOCOL found at Appendix D provides a template of a data protection protocol created by the Author to provide guidance to arbitrators when addressing these issues under the GDPR in international commercial arbitration cases.

stipulation, or tribunal order (all of which will be referred to herein for simplicity as "data protection protocols" or "protocols"). Depending on the facts, these protocols are likely to cover, among other things, transparent data processing information (potentially including data privacy notices), cybersecurity, third country data transfers, data breach notifications, and the allocation of roles and responsibilities with respect to compliance with the data subject's other rights.[240] These protocols will typically be signed and confirmed by everyone receiving Personal Arbitral Data during the course of the arbitration to insure compliance and will often impact the taking of evidence.[241]

It is preferable for the parties to agree a reasonable data protection protocol, taking into consideration the views of the arbitrators and the institution that will also have to apply them.[242] This process of agreeing a data protection protocol involves understanding the applicable data protection laws, the types and importance of the data being exchanged, the cybersecurity systems and capabilities of all the Arbitral Data Custodians that will be receiving and processing Personal Arbitral Data, the risks if the data were to be exposed, *etc*. Where parties are not able to agree reasonable data protection measures, tribunals will be asked to assist in this process and ultimately to decide where agreement is not possible.[243]

This is further impacted by the fact that the IBA Guidelines and other rules and protocols potentially applicable to data disclosure in international arbitration do not expressly address how the data protection rules may impact an arbitration, nor do the data protection rules (including the GDPR) contain express provisions addressing their application to international arbitration. While each set of rules may contain provisions that could be used to reconcile the two systems, they are not explicit about their relationship to each other. To leave this for a case-to-case determination allows for tailoring the process given the multitude of conflicting rules applicable to arbitral disclosure and data protection worldwide. However, it also creates significant uncertainty and leaves parties, external counsel,

240. *See* SEDONA PROTOCOL, *supra* note 76, at Appendix C to this Article (addressing discovery for litigation only); *see also* ARBITRAL DATA PROTECTION PROTOCOL, Appendix D.

241. *See id.*

242. *See* ICCA Cybersecurity Protocol, *supra* note 202, art. 13, at 13 (addressing cybersecurity only).

243. *See id.*, at art. 14, at 13 (addressing cybersecurity only).

institutions and arbitrators with the unenviable task of considering in each case how the data protection rules may limit the ways in which they can gather, process, use, transfer, and protect Personal Arbitral Data and the means by which the rights granted to data subjects will be complied with.

In practice, data protection protocols will be agreed to help maximize arbitral efficiency while minimizing data protection risks. This is a highly case specific enquiry, and is likely to lead to different rules being applied in each case and within the same case for different Arbitral Data Custodians and even between data sets. But if properly analysed early in the process, reasonable compliance measures can be put in place to minimize these risks without significantly impacting the arbitral process. Further, while it is beyond the scope of this Article to address liability, the protocol may need to include indemnification provisions where the original data processors agree to comply with the data subject rights (for example, data transparency potentially including data privacy notices) on behalf of other Arbitral Data Custodians (for example, the institution and/or the arbitrators).

This is consistent with the approach adopted by the IBA Rules. While not addressing data protection specifically, the IBA Rules provide in the newly added Article 2 that:

> 1. The Arbitral Tribunal shall consult the Parties at the earliest appropriate time in the proceedings and invite them to consult each other with a view to agreeing on an efficient, economical and fair process for the taking of evidence.
>
> 2. The consultation on evidentiary issues may address the scope, timing and manner of the taking of evidence, including:
>
> . . . .
>
> (c) the requirements, procedure and format applicable to the production of Documents;
>
> (d) the level of confidentiality protection to be afforded to evidence in the arbitration; and
>
> (e) the promotion of efficiency, economy and conservation of resources in connection with the taking of evidence. [244]

The Official Commentary on the IBA Rules explains that the addition of a mandatory conference on evidentiary issues early in the proceedings was intended to address the needs posed by increasingly

244. IBA Rules, *supra* note 7, art. 2, at 6.

large and complex arbitrations to ensure that evidentiary issues are addressed in a manner that promotes efficient and fair proceedings. [245] The items listed for discussion are not intended to exhaustive. [246] The extent to which data protection issues may impact the taking of evidence fits within the types of issues to be addressed early, and if the parties do not put this on the agenda for the procedural conference, the tribunal should do so as the data protection rules potentially apply to the tribunal itself and other Arbitral Data Custodians beyond the parties (and to avoid surprises later).[247] In addition to minimizing general data protection risk, this practice fosters compliance and encourages data protection concerns to be voiced at the outset, rather than later on in the proceedings (for example in response to a disclosure request), which could create delays. Further, by giving the parties the opportunity to plan the arbitral process from the outset in a way that minimizes data protection risks, parties are limited in their ability to later claim that these issues were not properly taken into consideration.

b. Document Disclosure

The IBA Rules foresee in Article 3 a system for the voluntary exchange of data between the parties and as ordered by the tribunal when the parties cannot agree.[248] The GDPR requires among other things that that the processing of personal data be minimized.[249] This may impact the amount of documentary evidence to be reviewed and exchanged during the course of the arbitration both voluntarily and as ordered by the tribunal, as well as the evidence submitted to the tribunal. Minimizing the amount of data exchanged in compliance with the GDPR will be assisted by early tribunal input as to the extent and nature of the proof to be submitted in support and defense of the claims. In high value complex disputes, the parties will be inclined to submit as much proof as possible through extensive document review of their own documents and those obtained from the other side, but

245. *See* COMMENTARY ON THE REVISED TEXT OF THE 2010 IBA RULES ON THE TAKING OF EVIDENCE IN INTERNATIONAL ARBITRATION, at 6 (2010) [hereinafter IBA COMMENTARY ON RULES].

246. *Id.*

247. *See*, *e.g.*, ICCA Cybersecurity Protocol, *supra* note 202, art. 14.

248. *See* IBA RULES, *supra* note 7, art. 3.

249. *See* GDPR, *supra* note 2, art. 17, rec. 65, at 12.

this may increasingly need to be tempered by data protection concerns, including data minimization.

The process foreseen by the IBA Rules provides that each party shall first submit their reliance documents, followed by any production requests for documents from the opposing party. With respect to the production of documents from the opposing party, Article 3 (3) of the IBA Rules[250] provides that a Request to Produce should contain:

> (a) (i) a description of each requested Document sufficient to identify it, or
>
> (ii) a description in sufficient detail (including subject matter) of a narrow and specific requested category of Documents that are reasonably believed to exist; in the case of Documents maintained in electronic form, the requesting Party may, or the Arbitral Tribunal may order that it shall be required to, identify specific files, search terms, individuals or other means of searching for such Documents in an efficient and economical manner;
>
> (b) a statement as to how the Documents requested are relevant to the case and material to its outcome; and
>
> (c) (i) a statement that the Documents requested are not in the possession, custody or control of the requesting Party or a statement of the reasons why it would be unreasonably burdensome for the requesting Party to produce such Documents, and
>
> . . .
>
> (ii) a statement of the reasons why the requesting Party assumes the Documents requested are in the possession, custody or control of another Party.

When objections to the production are raised:

> the Arbitral Tribunal shall then, in consultation with the Parties and in timely fashion, consider the Request to Produce and the objection. The Arbitral Tribunal may order the Party to whom such Request is addressed to produce any requested Document in its possession, custody or control as to which the Arbitral Tribunal determines that (i) the issues that the requesting Party wishes to prove are relevant to the case and material to its outcome; (ii) none of the reasons for objection set forth in Article

250. IBA RULES, *supra* note 7, art. 3.

> 9.2 applies; and (iii) the requirements of Article 3.3 have been satisfied. Any such Document shall be produced to the other Parties and, if the Arbitral Tribunal so orders, to it.[251]

The question is what role data protection issues including data minimization should play in making this determination.

Article 9(2) of the IBA Rules provides further that:

> 2. The Arbitral Tribunal shall, at the request of a Party or on its own motion, exclude from evidence or production any Document, statement, oral testimony or inspection for any of the following reasons:
>
> (b) legal impediment or privilege under the legal or ethical rules determined by the Arbitral Tribunal to be applicable;
>
> (c) unreasonable burden to produce the requested evidence; [or]
>
> . . .
>
> (g) considerations of procedural economy, proportionality, fairness or equality of the Parties that the Arbitral Tribunal determines to be compelling. [252]

Article 9(2) provides that an arbitral tribunal can exclude evidence because of a legal impediment. The Official Commentary to the IBA Rules explains that the legal impediment provision found in Article 9(2)(b) was geared at privileged documents and communications, rather than other legal impediments such as those contained in the GDPR.[253] However, the underlying principle could be applied to GDPR-related legal impediments. Furthermore, data protection restrictions could also be deemed to make the burden of producing the document unreasonable under (9(2)(c) and to be relevant to the tribunal's consideration under 9(2) (g) of "procedural economy, proportionality, fairness or equality of the Parties that the Arbitral Tribunal determines to be compelling." [254]

Going forward under the GDPR, one can expect that data protection considerations will increasingly be raised in deciding on disclosure requests. This will require a balancing of the requesting party's need for the documents against the data protection risks created and reasonable means to limit those risks.[255] This will

---

251. *Id.*
252. *Id.* art. 9(2), at 19.
253. *See* IBA COMMENTARY ON RULES, *supra* note 245, at 25.
254. IBA RULES, *supra* note 7, art. 9, at 19.
255. *See generally* GDPR, *supra* note 2, Rec. 4, at 2.

typically include establishing a data protection protocol that will form the basis for the disclosure as well as the other processing of Personal Arbitral Data. WP29 has said in the context of US litigation discovery that data protection concerns favor limiting data disclosure as much as reasonable by undertaking local data review and scrubbing before data is disclosed or transferred outside the European Union, as well as pseudonymization where possible.[256] However, the narrowly focused nature of disclosure in international arbitration means that the data disclosure requests will be much more limited. Furthermore, the arbitral process is often confidential (or can be made so), which means that the risks created by disclosure are minimized compared with the use of data in court proceedings.

Issues to be considered by the tribunal in balancing these competing concerns may include, among other things, procedures for limiting the data protection exposure though data protection protocols and other procedures limiting the risks, reasonable measures to avoid unnecessary third country data transfers, the objecting party's previous treatment of the data, pseudonymization where feasible, the scope of the compliance risk, and the importance of the data for the arbitration. In deciding these issues, the GDPR applies a risk-based analysis to compliance based on proportionality (as also set forth in Article 9(2)(g) of the IBA Rules above) and taking into account "the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons."[257] WP29 has already taken the express view that parties "have a legitimate interest in accessing information that is necessary to make or defend a claim, but this must be balanced with the rights of the individual whose personal data is being sought."[258]

It is beyond the scope of this Article to address liability issues or how data protection might impact enforcement of the award. However, in measuring the risk of non-compliance, the tribunal will be cognizant of the fact that the GDPR will be enforced primarily by Member State supervisory authorities acting as independent agencies with the authority to investigate and issue significant fines and criminal sanctions, and further that each data controller is independently liable for infractions.[259] With serious GDPR violations

256. Disclosure Guidelines, *supra* note 75, at 12.
257. GDPR, *supra* note 2, art. 24(1), at 47.
258. Disclosure Guidelines, *supra* note 75, at 1.
259. *See* GDPR, *supra* note 2, art. 58, at 69.

(including unlawful transfer) carrying fines of up to EU€20 million or four percent of annual global gross revenue, supervisory authorities carry significant clout, which risk will need to be taken into account in addressing these issues by the parties, their counsel, and the tribunal.[260]

V. CONCLUSION

The GDPR is of potential application to virtually all data processing in arbitrations with a nexus to the European Union. The GDPR imposes extensive requirements on the processing of data during an arbitration which are challenging to apply in the arbitral context in that they apply across the board to virtually everyone in the process and create overlapping rights and duties. Furthermore, both third countries and all twenty-eight Member States are likely to have somewhat different data protection laws as they apply to arbitration given that the GDPR allows for derogations, some of which apply to arbitrations. The reality is that determining the matrix of data protection laws potentially applicable to a dispute will itself be a complex exercise and will likely result in the application of many countries' laws to the same dispute and the various Arbitral Data Custodians, which could also create overlapping and conflicting obligations (and significant confusion). However, notwithstanding these difficulties, all Arbitral Data Custodians covered by the GDPR should make good faith efforts at compliance because the data protection rules established in the GDPR are of mandatory application and the risk of noncompliance is steep.

Interestingly, while these issues have been considered extensively in the context of litigation, international arbitration is virtually a green field.[261] The reasons for this are unclear and are likely to be numerous, but the lack of attention may stem in part from the fact that the expansion of data protection laws has been led by the European Union, which, until recently, has for the most part avoided international arbitration. This has now changed and the European Union is highly focused on arbitration at least in the investor-State context. At the same time, the GDPR has become a compliance imperative on par with antitrust and anticorruption for the companies that use international arbitration services. Over time, these companies

260. *See, id.,* art. 83, at 82.

261. See, Burianski & Reindl, *supra* note 15 (taking the same view).

will likely make data protection compliance an imperative for international arbitration in the same way they have for the other aspects of their businesses. Moreover, arbitrators and other Arbitral Data Custodians will all be concerned about their own liability, which itself will create a further compliance incentive.

In deciding what this means in practice, the Sedona Protocol and the Disclosure Guidance issued by WP29 in the context of discovery for US civil litigation provide useful starting points for addressing data protection compliance in international commercial arbitration. However, the issues raised by wide-ranging US discovery demands and the limited data disclosed during an international arbitration are obviously different. In addition to the more limited scope of disclosure in international arbitration, relevant differences include the fact that arbitration is a consensual process based in contract. Further, international commercial arbitration is often confidential, or could be made so, which further lowers the data protection risk.

As addressed herein, this will all need to be taken into account in applying the GDPR to international arbitration. When obligations conflict, decisions will have to made about how to comply, which should reflect a reasonable good faith effort to comply with GDPR principles and to protect the data subject's rights in line with those principles, within the constraints of the arbitral process and the requirements of due process. The role of the parties, their counsel, and the tribunal is to undertake a careful and practical analysis of the need for the data. This need for the data will then need to be balanced against the data protection risks and how those risks might be mitigated taking into account proportionality. As set forth in Appendix D, this should be reflected when designing and implementing a reasonable data protection protocol and deciding disclosure requests within the context of an arbitration, while at the same protecting the due process rights of the parties.

The arbitration community should consider whether to engage proactively with the European Data Protection Board (which will replace WP29) and/or Member State supervisory authorities, to address these issues proactively, keeping in mind that, while clarity is preferable, it may come at a price in terms of compliance obligations. One possibility would be the development of an approved Code of Conduct for data processing in international arbitration. The European Union has strongly encouraged the development of such codes generally, which the European Commission has said in the context of

third country data transfers are intended to "allow the development of more tailor-made solutions for international transfers, reflecting, for instance, the specific features and needs of a given sector or industry, or of particular data flows." Under the DP Directive only one code of conduct has ever been approved, but the European Commission would like this to change under the GDPR.[262] However, this will remain a time consuming and arduous process with an uncertain outcome. However, the current uncertainty, combined with the increased compliance risk to all Arbitral Data Custodians, may mean that they will err on the side of caution in ways that are even more damaging to the arbitral process.

In sum, the application of the GDPR to international commercial arbitration will be challenging. It is therefore fortuitous that one of arbitrations many strengths is its flexibility. This should enable the GDPR to be applied to arbitration in a manner that respects both the data subject's rights under the regulation and the parties' rights in the arbitration, as well as the arbitrators' duties. This is subject to the provision that when applying the GDPR to international commercial arbitration the regulators respect its decision-making function, and recognize the cross border, consensual and potentially confidential nature of the arbitral process.

262. *See* Commission Communication, *supra n*ote 49; GDPR*, supra* note 2*,* arts. 40, 46, at 63-64, 69.

APPENDIX A

Data Protection Questions to Pose in Planning an Arbitration

1. Does the arbitration agreement address data protection?
2. What does the applicable data retention policy provide?
3. What does the data protection policy or agreements say about use of the data for dispute resolution?
4. Where is the data?
5. How will the data be collected? Who will collect the data?
6. What kind of data is it?
7. Is the data considered "personal data" or otherwise covered under applicable the data protection laws? If so, where?
8. Is any of the data "special category data" or covered by more stringent data protection laws?
9. Does the collection and use of the data for a potential arbitral claim or defense provide an adequate basis for processing the data under the relevant data protection laws? If not, what needs to be done to ensure compliance?
10. Is the amount of data being collected fair and proportionate to the claim? Have efforts been taken to minimize the amount of data collected? How and where will it be culled? Is pseudonymization feasible?
11. Is it required to send a data privacy notice informing the individual "data subjects" that their data is being collected for use in a potential arbitration or is this already covered by applicable data protection policies? Is this practically possible if data from many individuals are collected? What impact would notification have on any confidentiality of the proceedings (that may have yet to be brought)?
12. Does the proposed method of data collection and review provide adequate data security?
13. Does the data collection and review require the transfer to third countries, and, if so, is this transfer lawful?

14. What external counsel would be best for the case? Where are they located? Do they have an EU establishment? Are any data transfer restrictions implicated? How will travel be impacted?
15. What would be the preferred candidate for arbitrator? Where are they located? Do they have an EU establishment? What is their data infrastructure?

APPENDIX B

Data Protection Questions to Consider in Crafting the Arbitral Procedure

1. What kinds of Personal Arbitral Data will be processed during the arbitration?
2. Is any Personal Arbitral Data potentially covered by the GDPR or other applicable data protection laws? If so, where? What legal obligations are imposed under the GDPR, Member State law, or third country laws?
3. What kind of activities will be undertaken with the Personal Arbitral Data during the arbitration itself? Where will it be processed? How will it be culled? Who will undertake the data analysis? Is pseudonymization an option?
4. Does the Personal Arbitral Data include special categories of data under the GDPR or the laws or regulations of any other countries? Is it covered by any specific laws or rules (like HIPPA in the United States)?
5. How will any applicable data protection laws potentially impact the processing of the data during the arbitration? What is the legal basis for the processing?
6. How will any applicable data protection laws potentially impact the disclosure of the data for the arbitration? To opposing counsel and experts? The institution? The arbitral tribunal?
7. Will the data be transferred outside the European Union? Can the transfer of Personal Arbitral Data outside the European Union during the arbitral process be minimized? For example, should restrictions be placed on access to documents from outside the European Union? How will travel impact third country data transfer?
8. Are data privacy notices required and if so when? By whom? How will the data privacy notice or other communications with the data subjects address the specifics of the arbitral process (including arbitrator confidentiality)?

9. Before Personal Arbitral Data is transferred or disclosed during the arbitration, what should the disclosing party do to ensure compliance by the transferor with any applicable data protection laws? Will this be implemented through a data protection protocol by agreement or tribunal order?
10. Where is the party to which data may be disclosed located? If necessary could Personal Arbitral Data be lawfully transferred to (1) opposing party, (2) opposing counsel, (3) any experts, (4) the arbitrator(s), (5) the arbitral institution, and (6) amongst arbitrators? What and how will adequate safeguards be implemented?
11. What responsibilities does the party to whom Personal Arbitral Data is disclosed have under the law? By agreement? Through a data protection protocol?
12. What cybersecurity and other legal requirements should be imposed on the processing of Personal Arbitral Data during the arbitration?
13. What rights does the data subject have and how will these rights be respected? To the extent that these rights are overlapping and apply to all the Arbitral Data Custodians, should the Initial Data Controllers (typically the parties) be allocated responsibility for compliance with those rights that require communication with the data subject (*e.g.,* transparency obligations (including any required data privacy and transfer notices), right to review and rectification, *etc*.)? If so, will indemnification obligations will be put in place in the case of breach?
14. What notifications apply if Personal Arbitral Data is breached?
15. Who is legally responsible if the cybersecurity and other legal requirements imposed on the processing of Personal Arbitral Data are violated?
16. What role should the arbitral tribunal play in addressing data protection issues? between the parties? The institution?
17. To what extent do these rules and obligations apply to the arbitral tribunal? The institution? Can this risk be minimized?

18. Will a data protection protocol be put in place? Who is responsible for preparing the protocol? Who will sign it? When should it be implemented?
19. Does the potential that the award may be made public during the enforcement stage limit the extent to which reference can be made to Personal Arbitral Data in the award? How should this be addressed?

APPENDIX C

The Sedona Conference Cross-Border
Data Safeguarding Process + Transfer Protocol

United States Discovery for Civil Litigation
INSTRUCTIONS

The Sedona Conference Cross-Border Data Safeguarding Process + Transfer Protocol (the "*Protocol*") has two interrelated purposes. First, it is an ease-of-reference guide that identifies common techniques used to achieve best possible legal compliance with conflicting U.S. eDiscovery rules and extra-U.S. Data Protection Laws when foreign data needs to be processed and transferred for the purposes of U.S. Litigation. Second, the *Protocol* creates a record that can be presented to those with regulatory responsibilities for Data Protection, evidencing the steps taken to best comply with Data Protection Laws. The *Protocol* must be customized to record fully the actions undertaken to maximize legal compliance and should include a detailed explanation of the circumstances and factors taken into account. The following instructions should be used with the chart below:

1. Explain the reasons for preserving or collecting the data. Identify clearly the U.S. proceedings for which the Protected Data is processed and transferred. If the Protected Data is to be preserved or collected for reasons other than litigation, identify the legal proceeding requiring the processing and transfer.
2. Determine whether data required to be preserved, processed, or disclosed in the U.S. is subject to Data Protection Laws and, if so, which laws apply. Assess whether alternative, non-protected, sources of that relevant data exist. To the extent possible, produce non-protected sources of data, making production of relevant Protected Data less necessary. Determine the sources of relevant Protected Data, the methods of preservation, if it has been or will be further processed, and where it will ultimately be transferred.
3. Describe measures taken to minimize the processing and transfer of Protected Data, explaining the methodology

used to filter and eliminate irrelevant Protected Data. These culling activities may begin with a questionnaire or an in-person interview, followed by iterative use of software tools and other processes, creating a subset of relevant and necessary Protected Data for disclosure. Consider compiling Protected Data locally or in a country that is not subject to the transfer restrictions under the applicable Data Protection law. Identify categories of Protected Data potentially affected by the applicable Data Protection Laws.

4. Describe the various categories of Protected Data that will be processed or transferred by type, including personal and sensitive personal data, trade secrets data, restricted data, consumer data, state secrets, etc.
5. If appropriate, consider using the Model U.S. Federal Court Protective Order .. or similar protective orders, or stipulations with data protection language providing agreed-upon or court-ordered restrictions on the use, disclosure, and dissemination of Protected Data. Consider including options to redact and designate Protected Data as "Confidential" or "Highly Confidential." Further, consider restrictions related to the onward transfer of data once it reaches the U.S.
6. Strive to provide a transparent processing and transfer protocol to the Data Subjects, identifying impacted Data Subjects and the means to communicate to them the purpose for the processing and transfer of Protected Data, the categories of Protected Data at issue, the duties and obligations attendant to that Protected Data, data protection measures that will or have been put in place, and such other factors as may be required or appropriate under the circumstances. Such communications to Data Subjects may include postings, one-on-one meetings, group presentations, or notice and acknowledgement documentation requesting consent and providing question and answer information, in writing or orally, in both English and the local language.
7. Identify steps taken to secure Protected Data by describing the protective measures undertaken by the Data Controller, including, for example, agreements with

third parties, use of a protective order, the nature and type of encryption at rest and in transit, limitations on access to the Protected Data, and any other means of securing the Protected Data. Also describe procedures for responding in the event of a data breach.

8. Describe the efforts undertaken if notice is contemplated or required. Others to be consulted may include the Data Controller's data protection personnel such as data protection officers, data protection authorities with jurisdiction over the Protected Data, or local company organizations such as works councils.
9. Identify mechanism(s) used to legitimize the transfer of Protected Data. For the EU, depending on the U.S. recipient and transfer purpose, these mechanisms typically include the use of Binding Corporate Rules (intra-group transfers only), the new Privacy Shield certification,[263] Model Contracts, or some other means of satisfying transfer safeguard requirements.
10. Document procedures used to destroy or return Protected Data to the Data Controller when it is no longer necessary.
11. Consider identifying those responsible for overseeing preservation, processing, and transfer of the Protected Data and obtaining their signatures to signify that the steps recorded were in fact taken.

263. The new EU/U.S. Privacy Shield came into effect on June 12, 2016, with certification available since August 1, 2016 (*Commission Implementing Decision of 12.7.2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield*, COM (2016) 4176 final (Dec. 12, 2016), *available at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf [https://perma.cc/N2HT-V2B6] (archived May 30, 2018), replacing the old EU-US Safe Harbor certification after the Commission decision on which it was based was declared invalid by the Court of Justice of the European Union on October 6, 2015.

The Sedona Conference Cross-Border Data Safeguarding Process + Transfer Protocol United States Discovery for Civil Litigation	
ACTION ITEM	**INFORMATION**
1. Purpose for processing and transfer of Protected Data	Identify the type of legal proceeding for which Protected Data is being processed or transferred (e.g., reasonably anticipated or active civil litigation; government investigation; subpoena) with specific identification information (e.g., case name, docket number, filing location, filing date, description of legal proceeding).
2. Data Protection Laws at issue and specific sources of Protected Data	Identify the country whose Data Protection Laws are at issue, the specific Data Protection Laws implicated, and the significance of each; identify the location of the Protected Data, where it is processed, and the location to which it will be transferred.
3. Measures taken to minimize the processing and transfer of Protected Data	Explain methodology used to narrow and cull Protected Data for processing and transfer purposes to include only relevant and necessary material (e.g., use of preliminary questionnaires and interviews; use of technology and processes to de-duplicate and apply iterative searches; filter and compile information in a country not subject to transfer restrictions under the applicable Data Protection Laws).
4. Categories of Protected Data processed and transferred	Identify categories of Protected Data processed and transferred (e.g., information that is likely to identify the Data Subject, sensitive personal data, trade secret data, restricted data).

5. Limitation on use and dissemination of Protected Data	Identify stipulations or protective orders and their material terms or attach a copy (e.g., *Model U.S. Federal Court Protective Order*; general protective order; confidentiality agreement; Data Protection stipulation).
6. Transparency of processes and transfers concerning Protected Data	Identify steps taken (if and as appropriate or feasible) to make information available or to notify Data Subjects of processing, transfer, and onward transfer of Protected Data (e.g., internal communications; posted notice).
7. Steps taken to secure transferred Protected Data	Identify steps taken to secure Protected Data (e.g., third-party agreements, nature and type of encryption, password protection, access limitation and control).
8. Compliance with notification obligations (if any) to others with oversight of data protection	Identify others involved or who may need to be consulted with responsibility for Data Protection implementation (e.g., the company's data protection officer or works council; government data protection authority); explain their involvement and means of notification.
9. Bases upon which Protected Data is transferred	Identify Protected Data transfer mechanisms relied on for each U.S. recipient (e.g., EU/U.S. Privacy Shield Certification, EU Model Contract Clauses, Binding Corporate Rules, or other means of satisfying transfer safeguard).
10. Disposition of transferred Protected Data when no longer needed	Describe disposition of processed and transferred Protected Data (e.g., destruction or return of Protected Data) when no longer needed to fulfill obligations of the specific matter.
11. Person responsible for transfer and processing of Protected Data	Consider identifying the person or persons ultimately responsible for processing and transferring Protected Data and requiring their signed acknowledgement that the steps recorded have been taken.

APPENDIX D

Template Data Protection Protocol for Arbitrators
Background

When the GDPR applies to an arbitration, compliance inevitably requires the adoption of a data protection protocol. The highly regarded SEDONA PROTOCOL[264] set forth in Appendix C of this Article was developed in the context of data transfer for the purposes of discovery for US litigation. The principles contained in the SEDONA PROTOCOL are relevant to disclosure for purposes of international arbitration. However, given that it was adopted in the context of cross border discovery for United States litigation, it requires modification when applied to disclosure for international arbitration.

To assist arbitrators in this process, this ARBITRAL DATA PROTECTION PROTOCOL proposes a template for arbitrators to use as a guideline in developing a data protection protocol for use in international commercial arbitrations governed by the GDPR. Like the SEDONA PROTOCOL, it is intended to provide "an ease-of-reference guide that identifies common techniques used to achieve best possible legal compliance with conflicting" requirements for data processing in international arbitration covered by the GDPR, and at the same time creating "a record that can be presented to those with regulatory responsibilities for Data Protection, evidencing the steps taken to best comply with applicable data protection laws."[265] While the parties may adopt a broader data protection agreement, this template is geared towards the issues that will typically need to be addressed during the arbitral process itself. It will require customization on a case-by-case basis to demonstrate the steps taken to comply with the GDPR and an explanation of the circumstances and factors taken into account in constructing the protocol. The principles set forth in this Article[266] and the instructions described Appendix C with respect to the SEDONA PROTOCOL will be helpful in applying the concepts set forth in this ARBITRAL DATA PROTECTION PROTOCOL.

---

264. *See* SEDONA PROTOCOL, *supra* note 77, Appendix C of this Article.

265. *Id.*

266. Kathleen D. Paisley, *It's all About the Data: Impact of the EU General Data Protection Regulatio*n, 41 FORDHAM INT'L L.J. 841 (2018)

Template Data Protection Protocol for Arbitrators[267]	
ACTION ITEM	**INFORMATION**
Data controllers and processors	Identify who will act as controllers and processors of Personal Arbitral Data during the arbitration. Each data controller and processer should sign the ARBITRAL DATA PROTECTION PROTOCOL. Identify the Initial Data Controller who engaged in the original processing of the data (typically a party to the arbitration) and who will be responsible in the first instance for complying with certain data subject rights. Consider the additional obligations of the Initial Data Controllers and any indemnities they should provide to the other secondary controllers. If relevant, identify others who may need to be consulted with responsibility for data protection implementation; explain their involvement and means of notification.
Member State Exemptions	Identify any Member State exemptions being replied upon to limit the data subject rights and which controllers are covered by such exemptions.
Categories of Personal Arbitral Data to be processed during the arbitration	Identify categories of Personal Arbitral Data that will be processed and transferred during the arbitration (*e.g.*, types information that is likely to identify data subjects (emails, lab notebooks, agreements, construction logs, pleadings, witness statements, awards, *etc*. and special category data), as well as commercially sensitive and/or restricted or highly confidential data.

267. Originally promulgated by the Sedona Conference, and adapted by the Author for use in international commercial arbitrations governed by the GDPR.

Legal basis for the processing	Identify the legal basis for the processing (typically the legitimate interests of the controller) and what has been done to comply with the requirements imposed by the GDPR[268] on processing for that purpose. If special category data will be processed, provide justification for the processing of that data.
Third-country data transfer	Identify whether any Personal Arbitral Data will be transferred outside the European Union and the legal basis for the transfer (usually the legal claims exemption and/or the legitimate interests of the data controller). Identify what has been done to comply with the legal requirements including notice that may be imposed on transfer. Identify the means by which data may be transferred outside the European Union and whether Personal Arbitral Data can be downloaded, emailed, or stored on computers outside the European Union. Consider the impact of travel on data transfer.
Confidentiality	Identify whether the arbitral process will be confidential and consider entering into confidentiality agreements addressing specific issues. Consider the confidentiality of the award and whether it can/should be redacted to ensure that Personal Arbitral Data will not be made public. Address the confidentiality of arbitrator communications within the tribunal and with the institution.

268. All references in this ARBITRAL DATA PROTECTION PROTOCOL to the GDPR should be deemed to include applicable Member State laws implementing the GDPR.

Cybersecurity	Identify the cybersecurity measures that will be employed to protect the data, including the principles discussed in GDPR and the ICCA Cybersecurity Protocol to the extent consistent with the GDPR (*e.g.*, use of the cloud, nature and type of encryption, password protection, access limitation and control, *etc*.). Consider the impact of travel and how Personal Arbitral Data can be stored or retrieved during travel outside the European Union.
Data Minimization	Identify the steps to be undertaken to ensure that only relevant and necessary data is processed during the arbitration. Explain the methodology to be applied to narrow and cull Personal Arbitral Data for processing and transfer during the arbitration to include only relevant and necessary material (*e.g.,* use of preliminary questionnaires and interviews; use of technology and processes to de-duplicate and apply iterative searches; identification and elimination of special category data where possible, consideration of pseudonymization where possible, filtering and compiling information in an EU country, *etc*.)
Transparency/Data Privacy Notices	Identify what steps are required to make information available to data subjects about the processing, transfer, and onward transfer of Personal Arbitral Data for purposes of the arbitration (*e.g*., internal communications; posted notice). Consider whether additional data privacy notices may be required. Consider whether the Initial Data Controller should be primarily responsible for meeting such transparency requirements and providing any required notices. Consider whether the Initial Data Controller should indemnify the other secondary controllers for failure to provide adequate notice or other rights under its control. Address the

	confidentiality of arbitrator communications within the arbitral tribunal and with the institution and the impact this has on transparency obligations.
Data rectification, erasure, and no further processing	Identify what steps will be undertaken if a data subject exercises its right to rectify, erasure or stop processing of its Personal Arbitral Data. Confirm whether the Initial Data Controller should be primarily responsible for addressing such requests in the first instance and consider how the tribunal will be informed of the request and if the data has been altered as a result. Consider whether the Initial Data Controller should indemnify the other secondary controllers for failure to comply with the data subject rights under its control.
Data retention	Describe how long data will be retained for purposes of the arbitration and how it will be disposed of (*e.g.*, destruction or return of Personal Arbitral Data) when no longer needed to fulfill obligations of the controllers of the data. The disposal date is likely to differ for each controller given their legal and ethical retention obligations.
Data Breach Notices	Identify the exact process that will be undertaken if a data breach occurs, and the notification deadlines imposed taking into account the very strict 72-hour deadline established in the GDPR for informing the relevant supervisory authorities. Describe exactly what will be considered a data breach.
Indemnification	Consider whether the Initial Data Controllers should provide indemnities to the other secondary controllers for failure to comply with mandatory data subject rights.