

## **Data Protection and International Arbitration: how to make these two different worlds coexist in the digital era**

**Direito da Proteção de Dados e Arbitragem Internacional: como fazer estes dois mundos coexistir na era digital**

**Diana Camões**

Parliamentary Advisor at the Portuguese Parliament. Master's in International and European Law Porto Faculty of Law – Catholic University of Portugal (currently waiting for the Dissertation's defense), Postgraduate degree in Data Protection Law at the Private Research Law Center – Lisbon Faculty of Law

R. de Diogo Botelho 1327, 4169-005 Porto, Portugal

diana.camoes@hotmail.com

<https://orcid.org/0000-0001-8827-007X>

February 2024

**ABSTRACT:** This study aims to reflect on the importance of data protection law, namely the General Data Protection Regulation (GDPR), when it comes to International Arbitration, which is something that implies the need to articulate different laws and international treaties. For this reason, we address the different issues regarding the material and territorial scope of the regulation, as well as the question of transfers of personal data to third countries. We also analyze which personal data can be processed during an international arbitration. Finally, our investigation takes into consideration some of the main issues regarding the proceeding of arbitration itself and evaluates whether the GDPR can offer, when applicable, a coherent answer to the data protection's issues emerging in international arbitration. In a world more technologic than ever, this study aims to demonstrate how these two different worlds (data protection law and international arbitration) can collide for a common application whenever it is necessary.

**KEY WORDS:** Data protection; general data protection regulation; arbitration; international arbitration; personal data; technology.

**RESUMO:** O presente artigo tem como objetivo refletir sobre a importância do direito da proteção de dados, nomeadamente o regulamento geral da proteção de dados (RGPD), na arbitragem internacional, algo que implica conciliar leis e tratados internacionais distintos. Por essa razão, abordamos os problemas relativos ao âmbito de aplicação material e territorial do regulamento, bem como a questão das transferências internacionais de dados pessoais para países terceiros. Analisamos, igualmente, quais os dados pessoais que podem ser tratados num contexto de arbitragem internacional. Finalmente, a nossa investigação toma em consideração os principais problemas relativos ao procedimento arbitral e avalia se o RGPD pode oferecer, quando aplicável, uma resposta coerente para os problemas de direito da proteção de dados pessoais que surgem no contexto da arbitragem internacional. Num mundo mais tecnológico do que nunca, o presente estudo procura demonstrar como poderão dois mundos tão distintos (direita proteção de dados pessoais e arbitragem internacional) colidir para uma aplicação comum sempre que se torne necessário.

**PALAVRAS-CHAVE:** Proteção de dados; regulamento geral de proteção de dados; arbitragem; arbitragem internacional; dados pessoais; tecnologia.

## **SUMMARY:**

1. Introduction
  2. The applicability of the GDPR
    - 2.1. Material Scope of the GDPR
    - 2.2. Territorial Scope of the GDPR
    - 2.3. Transfers of Personal Data to third countries
  3. Specific issues regarding the Arbitral Proceeding
    - 3.1. Online Hearings
    - 3.2. Evidence
    - 3.3. Refusal of the Award on the Basis of the GDPR's violation
  4. A data protection agreement as a path to follow?
  5. Conclusion
- Bibliography
- Relevant Documents
- Cases
- Legislation

## 1. Introduction

International Arbitration<sup>1</sup> is not immune to the different challenges posed by this new era of digitalization. Not only “modern international society and commerce are characterized by a complex, and sometimes disordered web of interrelationships”<sup>2</sup>, as well as it is necessary to adapt its system to the different issues arising. Regardless, even though international arbitration is not “a flawless system”<sup>3</sup>, this does not mean that it is void of advantages.<sup>4</sup> Thus, we live in a world where data is considered to be “the new oil”<sup>5</sup> and, for that reason, new divergent regulations have been created. The prime example is the General Data Protection Regulation (“GDPR”)<sup>6</sup>, which is considered to be the leading legislation in data protection law. Therefore, with different treaties side to side<sup>7</sup> and reinforced data protection rules, especially in the European Union (“EU”) when compared to other countries<sup>8</sup>, new challenges are arising in how to apply (or not) these rules to international arbitration proceedings’, leading some to consider this “the clash of the titans.”<sup>9</sup>

Even if the EU is considered to be the role model on this subject, we cannot ignore that other countries have adopted its own regulations.<sup>10</sup> This issue is recent, but not completely ignored by the authorities in regards to arbitration. In fact, the International Council for Commercial

<sup>1</sup> Investment Treaties are celebrated between two or more states according to which contracting state agrees to receive investors in accordance to some standards of protection.

<sup>2</sup> As it is prescribed by ZACHARY DOUGLAS, “The Hybrid Foundations of Investment Treaty Arbitration”, in *British YearBook of International Law*, Volume 74, Issue 3, 2003, pp. 151-289(203).

<sup>3</sup> FILIPE GALVÃO TELES SANCHES AFONSO, “The fifth arbitrator? The Role of Artificial Intelligence to Tribunals in International Arbitration”, in *Revista Internacional de Arbitragem e Conciliação*, Volume XIII, 2020, pp. 147-188(148).

<sup>4</sup> Overall, it is an efficient, flexible system and less expensive. Vide MAFALDA MIRANDA BARBOSA, “Do Juiz Árbitro ao software juiz árbitro: uma evolução possível?”, in *Revista Internacional de Arbitragem e Conciliação*, Volume XIII, 2020, pp. 37-64(37). On the other hand, SUSAN D. FRANCK, “The Legitimacy Crisis in Investment Treaty Arbitration: Privatizing Public International Law Through Inconsistent Decisions”, in *Fordham Law Review*, Volume 73, Issue 4, 2005, pp. 1521-1625(1524) also outlines one main key to the system, as it allows not only investors to obtain financial returns and gains in the markets of the future, as well as attract investment to countries, which is more important in those less developed.

<sup>5</sup> Even though this has to be seen from a metaphorical point of view. See DENNIS D. HIRSCH, “The Glass House Effect: Big Data, The New Oil and the Power of Analogy”, in *Maine Law Review*, Volume 66, 2014, pp. 373-495(379) states that if data is considered the new oil, then this “data releases are the new oil spills.”

<sup>6</sup> Regulation (EU) 2016/679 of the European Parliament of the Council, 27 April 2016.

<sup>7</sup> There are BITs or Bilateral Investment Treaties (some countries have their own model) and Multilateral Investment Treaties treaties or FTA with chapters dealing with investment [Comprehensive Economic and Trade Agreement (“CETA”), Canada-United States Mexico Agreement (“CUSMA”), North American Free Trade Agreement (“NAFTA”), Comprehensive and Progressive Agreement for Trans-Pacific Partnership (“CPTPP”), Energy Charter Treaty (“ECT”), among others].

<sup>8</sup> Besides the structural conflicts of EU Law and Bilateral Investment Treaties. Vide “Conflict Resolution between EU Law and Bilateral Investment Treaties of the EU Member States in the Aftermath of Achmea”, in *Yearbook of European Law*, 2023, pp. 1-27(1), available <https://doi.org/10.1093/yel/yeac012> (19.09.2023)

<sup>9</sup> NEVA CIRKVENI / PER NEUBURGER, “Clash of the Titans: GDPR and International Arbitration – A Look at the Future”, *Rechtsanwälte Attorneys Law*, 2021, available <https://oblin.at/publication/clash-of-the-titans-gdpr-and-international-arbitration-a-look-at-the-future/> (13.09.2023)

<sup>10</sup> As ANTÓNIO BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados à luz do RGPD e da Lei n.º 58/2019*, Coimbra, Almedina, Reimpressão, 2020, p. 53 remembers it was with the Special Subcommittee on Invasion of Privacy that the contemporary phase of Data Protection began.

Arbitration (“IBBA”) has published a *RoadMap to Data Protection in International Arbitration*<sup>11</sup>, which is a clear demonstration of the importance that the topic is starting to assume.

Are these two different worlds colliding? Due to technology’s preponderant role in every field of law, it is more important than ever to ensure a coherent approach. Therefore, this essay aims to analyze different points of crossover between these two branches of law and the main problems that might arise from the applicability of the GDPR. This is not so far a hot topic in the doctrine, even though it is possible to find a few written articles.<sup>12</sup> Consequentially, we will further reflect on (i) the possibilities of the application of the GDPR within the context of international arbitration (including the ones held outside the EU), (ii) which data is processed during these proceedings, (iii) the issue of virtual arbitration hearings, as well as electronic data and (iv) the use of the GDPR as a potential way to annul or refuse the enforcement of an arbitral award.

## 2. The applicability of the GDPR

Nowadays, as Kathleen Paisley outlines, “data processing is an essential component of modern international arbitration.”<sup>13</sup> Digitalization has led to the change of paradigm within different branches of law, which has resulted in “conflicting requirements, not only within the field of data protection itself but also between data protection regimes and other areas, e.g international arbitration.”<sup>14</sup>

There are no doubts on the impact that a strict regulation like the one foreseen on the GDPR, which is also the most known regime in data protection law, might have in dealing with these proceedings, due to the significant number of obligations and legal norms that have to be fulfilled. In order to assess the possibility of the application of the GDPR, we have to take into consideration two different scenarios: the material requirements and the territorial scope.

<sup>11</sup> INTERNATIONAL COUNCIL FOR COMMERCIAL ARBITRATION (ICCA) / INTERNATIONAL BAR ASSOCIATION (IBA), *Joint Task Force on Data Protection in International Arbitration – Roadmap to Data Protection in International Arbitration*, 2022, available <https://www.arbitration-icca.org/icca-reports-no-7-icca-iba-roadmap-data-protection-international-arbitration> (15.10.2023). INTERNATIONAL COUNCIL FOR COMMERCIAL ARBITRATION (ICCA) / INTERNATIONAL BAR ASSOCIATION (IBA) / NEW YORK CITY BAR / INTERNATIONAL INSTITUTE FOR CONFLICT PREVENTION & RESOLUTION, *Protocol on Cybersecurity in International Arbitration*, 2022, available [https://cdn.arbitration-icca.org/s3fs-public/document/media\\_document/ICCA-reports-no-6-icca-nyc-bar-cpr-protocol-cybersecurity-international-arbitration-2022-edition.pdf](https://cdn.arbitration-icca.org/s3fs-public/document/media_document/ICCA-reports-no-6-icca-nyc-bar-cpr-protocol-cybersecurity-international-arbitration-2022-edition.pdf) (15.10.2023).

<sup>12</sup> Even though there are some relevant texts on this matter that we’ll have the opportunity to closely analyze, namely: JIE JEANNE HUANG, “Conflicts and Tentative Solutions to Protecting Personal Data in Investment Arbitration”, in *The European Journal of International Law*, Volume 32, no. 4, 2021, pp. 1191-1220(1191), NEVA CIRKVENI / PER NEUBURGER, cit.; KATHLEEN PAISLEY, “It’s All about the Data: The Impact of the EU General Data Protection Regulation on International Arbitration”, in *Fordham International Law Journal*, Volume 41, Issue 4, 2018, pp. 841-936(841). JIE JEANNE HUANG / DAN XIE, “Data Protection Law in Investment Arbitration: Applicable or Not?”, in *Arbitration International* (forthcoming), pp. 1-47, 2021, available [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3763222](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3763222) (02.10.2023).

<sup>13</sup> KATHLEEN PAISLEY, cit., p. 845.

<sup>14</sup> ELENA MAZETOVA, “Data Protection Regulation and International Arbitration: Can There be Harmonious Coexistence (with the GDPR Requirements Concerning Cross Border Data Transfer?)”, in *Legal Issues in the Digital Age*, 2/2021, 2021, pp. 21-48(23).

## 2.1. Material Scope of the GDPR

According to article 2(1) of the GPDR, the regulation is applicable to the processing of personal data wholly or partly by automated means.<sup>15</sup> Focusing on the concept of personal data, article 4(1) defines it as “any information relating to an identified or identifiable natural person.” Thus, it is possible to point out four different elements: (i) any information<sup>16</sup>, (ii) relating to<sup>17</sup>, (iii) identified or identifiable<sup>18</sup> and (v) natural person.<sup>19</sup>

Thinking about International Arbitration, several types of personal data might be included on this. It is actually interesting, since the International Council for Commercial Arbitration-International Bar Association and International Bar Association (“ICCA-IBA”) give relevance not only to the GDPR, as well as to the Brazilian legislation<sup>20</sup>, by pointing out that under these regulations “a substantial portion of the information exchanged during a typical international arbitration is likely that qualifies as personal data.”<sup>21</sup> Almost everything will fall within the concept of personal data if the requirements are met<sup>22</sup>, being irrelevant that it is “contained in a business-related document.”<sup>23</sup> Nevertheless, this does not include data related to companies, because the aim of the GDPR is to protect individuals. Thinking about arbitration, as Kathleen

<sup>15</sup> Excluded are, in accordance to article 2(3), (i) activities that fall outside the scope of EU Law; (ii) processing carried out by member states which fall within the scope of Chapter 2 of Title V of the TEU; (iii) by a natural person in the course or purely personal or household activity; (iv) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

<sup>16</sup> Which means that any sort of information might be relevant for the application of the GDPR, which demonstrates the willingness to consecrate a broader concept, as the ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 4/2007 on the concept of personal data*, adopted on 20<sup>th</sup> June 2007, p. 6 recognized. On the other hand, for it to fall within the scope of this concept, it is not necessary that the information is true, because even when it is false it will be considered personal data (and that’s why there’s the right of assess and ratification). As A. BARRETO MENEZES CORDEIRO, “Dados Pessoais: conceito, extensão e limites”, in *Revista de Direito Civil*, Ano 3, Volume 2, 2018, pp. 297-321(301) remembers it includes any aspect related to the person, whether it is a familiar, social, private public, mental or physical information.

<sup>17</sup> As the ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 4/2007* cit., pp. 9-12, points out, “information can be considered to “relate” to an individual when it is about that individual.” On this matter, three different elements are identified (even though they don’t need to be cumulative, being rather alternative), namely: content, purpose and result. On this matter, A. BARRETO MENEZES CORDEIRO, “Dados Pessoais...” cit., p. 303 clarifies that there’s an intrinsic relation between the information and the individual. *Vide* also A. BARRETO MENEZES CORDEIRO, *Direito da proteção de dados...* cit., pp. 110-112.

<sup>18</sup> A person can be identified when, within the group of persons, “he or she is distinguished from all the members of the group.” Contrarily, as the ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 4/2007*, p. 12, outlines a person will be identifiable when “although has not been identified yet, it is possible to do so.” On this matter it is also important Recital 26. *Vide* GRAÇA CANTO MONIZ, *MANUAL DE INTRODUÇÃO À PROTEÇÃO DE DADOS*, Coimbra, Almedina, 2023, pp. 43-44.

<sup>19</sup> Which means that the protection of the GDPR is only attributed to human beings.

<sup>20</sup> Which has many similarities with the GDPR. Some even say that it was inspired by it.

<sup>21</sup> ICCA-IBA, *Joint Task Force on Data Protection* cit., p. 9.

<sup>22</sup> An important note that it is also outlined by ICCA-IBA, *Joint Task Force on Data Protection*, p. 9 is related to the definition of “personal information” under the California Privacy Act. Personal information means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.” (1798.140 (o)(1)). Therefore, as it is pointed out, the definition does not extent to personal public information (1798.140 (o)(2)), which means information that is lawfully made available from federal, state, or local government records. As mentioned by W. GREGORY VOSS / KIMBERLY A. HOUSER, “Personal Data and the GDPR: Providing a Competitive Advantage for U.S Companies”, in *American Business Law Journal*, Volume 56, Issue 2, pp. 287-344(291) these different definitions “regarding what information is subject to protection” makes it harder for USA’ companies to analyze privacy law in the EU.

<sup>23</sup> *Ibid*, p. 9.

Paisley outlines, this also might include witness statements, expert reports and the award itself, because they “are likely to identify individuals.”<sup>24 25</sup>

On the other hand, under Article 4(2) of the GDPR, processing<sup>26</sup> means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.<sup>27</sup> Once again, there is a broader definition and, as Kathleen Paisley affirms, “virtually any activity undertaken during an arbitration relating to documents is likely to be covered by the GDPR.”<sup>28</sup> The same is held in the ICCA-IBA’s reports, as it is also recognized that “most activities undertaken in a typical international arbitration are likely to constitute processing.”<sup>29</sup> From the interpretation of the different provisions, the GDPR is also applicable (in general) to arbitrations.<sup>30</sup> If it might be easier to establish its applicability to commercial arbitration, regarding non-commercial arbitrations, where bilateral and multilateral treaties are celebrated, it might be harder.<sup>31</sup>

There is also a problem that is very relevant to this topic. In fact, as we’ve had the opportunity to affirm, the GDPR clarifies that the regulation does not apply to the processing of personal data “in the court of an activity which falls outside the scope of Union Law.”<sup>32</sup> This provision must be interpreted strictly, as the ECJ (“European Court of Justice”) has stated.<sup>33</sup> On the other hand, Recital 16 gives as example activities concerning national security.<sup>34</sup> Thus, one of the most interesting cases is *Tenant Energy, LLC c. Canada*<sup>35</sup>, an international arbitration under NAFTA, whose applicable law was the 1976 United Nations Commission on International Trade Law (“UNCITRAL”) Arbitration Rules. *In casu*, the *Tenant* argued that the GDPR should be taken into account.<sup>36</sup> The Government of Canada rejected this request, as it argued that the

<sup>24</sup> KATHLEEN PAISLEY, cit., p. 863.

<sup>25</sup> MARTIN ZAHARIEV, “Mission (im)possible: Where GDPR Meets Commercial Arbitration”, in CHRISTIAN KLAUSEGGER, et. al. (ed) *Austrian Yearbook on International Arbitration*, Bern, C.H. BECK, 2020, pp. 3-21(4) also outlines this point, by stating that in International Commercial Arbitration, almost all information workflow will be included (the author gives the example of the exchange of legal correspondence between the parties, the tribunal and the arbitral institution and digital platforms for management of cases that include these personal data, among others). DAVID ROSENTHAL, “Complying with the General Data Protection Regulation (GDPR) in International Arbitration – Practical Guidance”, in *Asa Bulletin*, Volume 37, Issue 4, 2019, pp. 822-837(824) states that “any handling of e-mails, letters, contracts or other documents or piece of data that contains the name, an e-mail address that allows a reader to identify the individual mentioned is subject to the GDPR.”

<sup>26</sup> See European Court of Justice (ECJ), Lindqvist, 06/11/2003, C-101/01, where the court held that the act of referring, on an internet page, to various persons and identifying them by name or by other means constitutes processing of personal data.

<sup>27</sup> The Article continues and adds some examples, “such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”

<sup>28</sup> KATHLEEN PAISLEY, cit., p. 864.

<sup>29</sup> ICCA-IBA, *Joint Task Force on Data Protection* cit., p. 10.

<sup>30</sup> See Recitals 20 and 91 of the GDPR.

<sup>31</sup> ALEXANDER BLUMROSEN, “The Allocation of GDPR Compliance in Arbitration”, in José R. Mata DONA / NIKOS (ed.) *International Arbitration and EU Law*, Cheltenham, Edward Elgar Publishing, 2021, pp. 92-109(96)

<sup>32</sup> Article 2(2)(a) of the GDPR. Vide GRAÇA CANTO MONIZ, cit., p. 45.

<sup>33</sup> European Court of Justice (ECJ), Lindqvist, 06/11/2003, C-101/01, paragraph 42. the Court specified that it wouldn’t be appropriate to interpret the expression (under the former directive) as having a scope which would require it to be determined in each individual case whether the specific activity at issue directly affected freedom of movement between Member States.

<sup>34</sup> A. BARRETO MENEZES CORDEIRO, “Artigo 2.º”, in A. BARRETO MENEZES CORDEIRO (Coord.) *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Coimbra, Almedina, 2021, pp. 66-70(68).

<sup>35</sup> Permanent Court of Arbitration (“PCA”), *Tenant Energy, LLC v. Government of Canada*, no. 2018-54. See HERKE KRANENBORG, “Article 2 Material Scope”, in CHRISTOPHER KUNER / LEE A. BYGRAVE / CHRISTOPHER DOCKSEY (ed), *The EU General Data Protection Regulation (GDPR)*, Oxford, Oxford University Press, 2020, pp. 60-73(60).

<sup>36</sup> *Tenant Energy, LLC v. Government of Canada, Claimant’s E-mail to the Tribunal regarding the Application of the EU GDPR*, 2019, available <https://www.italaw.com/cases/7250> (20.10.2023).

country already addresses confidentiality issues in the proceedings and that the “potential application of the GDPR should not prevent arbitration from moving forward.”<sup>37</sup> Consequentially, the Claimant delivered its response to the tribunal<sup>38</sup> and made a compelling argument, as it outlined that one of the arbitrators had an EU establishment and, as a result, the GDPR would cover him, as he would be considered a processor and controller.<sup>39</sup>

Nevertheless, the Tribunal refused the application of the GDPR, as it considered that neither the EU nor its Member States were parties and would not, presumptively, come within the material scope of the GPDR.<sup>40</sup> Martin Zahariev argues that “having in mind that investment arbitration is transnational by its nature, it can reasonably be argued that the rules it is subject to go beyond national or even regional legislation such as the EU.”<sup>41</sup> The doctrine outlines some incoherences and issues that seem to derive from this position adopted. Some argue that the Tribunal’s perspective is not “consistent with the latter case law decided by the Court of Justice”, which requires that the provision should be interpreted strictly.<sup>42</sup> Hence, Jie Jeanne Huang considers that this is very “questionable.”<sup>43</sup> On the other hand, Emily Hay mentions an important point, in our opinion, which is related to the fact that the provision at stake is “essentially made for internal EU Law.”<sup>44</sup> Of course that we do not have any doubts about the fact that neither the EU nor its Member States are parties to NAFTA. Still, having in mind the strict interpretation made by the ECJ, only activities concerning public security, defense, state security and activities in areas of criminal law.<sup>45</sup> Could the Tribunal have followed this path, by considering that the simple membership of NAFTA could relate to one of these topics? This would lead us to another discussion.<sup>46</sup>

We cannot forget that one of the arbitrators was from the United Kingdom (“UK”), which was still a member of the EU at the time. As Kathleen Paisley clarifies “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.”<sup>47</sup> <sup>48</sup> Therefore, that arbitrator would

<sup>37</sup> *Tenant Energy, LLC v. Government of Canada, Respondent’s Letter to the Tribunal regarding EU GDPR*, 2019, available <https://www.italaw.com/cases/7250> (25.10.2023).

<sup>38</sup> *Tenant Energy, LLC v. Government of Canada, Questions and Claimant’s Response to the Tribunal GDPR Questions and Data Privacy Questions*, 2019, available <https://www.italaw.com/cases/7250> (26.10.2023)

<sup>39</sup> *Ibid*, p. 3.

<sup>40</sup> *Tenant Energy, LLC v. Government of Canada, Tribunal’s Communication to the Parties*, 2019, available <https://www.italaw.com/cases/7250> (29.10.2023).

<sup>41</sup> MARTIN ZAHARIEV, *cit.*, p. 6 considers that, having in mind that investment arbitration is transnational by its nature, “it can reasonably be argued that the rules it is subject to go beyond national or event legislation such as the EU Law.”

<sup>42</sup> JIE JEANNE HUANG / DAN XIE, *cit.*, p. 14. Jie Jeanne Huang, *cit.*, pp. 1207-1208.

<sup>43</sup> JIE JUANG HUANG, *cit.*, p. 1208.

<sup>44</sup> EMILY HAY, “The Invisible Arm of the GDPR in International Treaty Arbitration: Can’t we make it go away?”, in *Kluwer Arbitration Blog*, 2019, available <https://arbitrationblog.kluwerarbitration.com/2019/08/29/the-invisible-arm-of-gdpr-in-international-treaty-arbitration-cant-we-make-it-go-away/> (11.11.2023)

<sup>45</sup> These are all activities foreseen on titles V of VI of the TFEU.

<sup>46</sup> JIE JEANNE HUANG / DAN XIE, *cit.*, p. 14.

<sup>47</sup> KATHLEEN PAISLEY, *cit.*, p. 898.

<sup>48</sup> GEORGE A. BERMAN, “The Future of International Commercial Arbitration”, in C. L. LIM (ed) *The Cambridge Companion to International Arbitration*, Cambridge, Cambridge University Press, 2021, pp. 138-175(153). outlines that “even if only one of the arbitrators or one of the parties is to be bound by the GDPR, it is more than likely that the whole proceeding will somehow be affected by the rules and the application of the GDPR.” Nevertheless, this wasn’t the opinion of the tribunal.



always be considered a controller in accordance to article 4(7) of the GDPR<sup>49</sup>, due to the fact that there is processing of personal data on his own authority, which is “not based on instructions given.”<sup>50</sup> Even if the GDPR was not to be applied, being the arbitrator a UK’s national, the issue of applying the UK Data Protection Act 2018 should, at least, have been mentioned.<sup>51</sup> Thus, from this point of view, it seems that the direction chosen “raises more questions that it provides answers regarding GDPR’s applicability.”<sup>52</sup>

As Jie Jeanne Huang and Dan Xie clarify, having in mind that article 2 stands “as a prerequisite” to article 3, that is why tribunal did not even bother to analyze if this situation could have fallen within the territorial scope of the GDPR.

Another important case, even if it does not relate directly to EU Law, is *Elliott Associates v. Korea*<sup>53</sup>, where the Korean Government defended the application of Personal Information Protection Act (“PIPA”) whereas the other party was against it. This makes a considerable difference, as Elliott Associates wanted the full publication of the documents in the case, because, in their opinion, PIPA could not be applicable to the following case. It argued, therefore, that the Respondent did not explain correctly why the different actors should be qualified as controllers, as well as the information had lawfully been published in press articles and were in the public domain.<sup>54</sup> This issue was related to the transparency regime established in Korean-United States Free Trade Agreement (“KORUS”). Under Article 11.28 of the Agreement, protected information is considered to be “confidential business information or information that is privileged or otherwise protected from disclosure under a Party’s Law.” Therefore, having in mind that PIPA is Korea’s Law, the problem arose. The Permanent Court of Arbitration (“PCA”) began by pointing out that PIPA does not merely regulate the processing of personal information for purposes of operating personal information files by personal information controllers, as it also protects information relating to a living individual that makes it possible to identify by his/her full name.<sup>55</sup> Moreover, the PCA ended up concluding that PIPA had to be applicable to the case.

---

<sup>49</sup> They are also arbitral participants, as recognized by the ICCA-IBA, *Joint Task Force on Data Protection* cit., pp. 12-15. See also ANANYA BAJPAI / SHAMBHAVI KALA, “Data Protection, cybersecurity and International Arbitration: Can they reconcile?”, in *Indian Journal of Arbitration Law*, Volume 8, Issue 2, 2020, pp. 1-18(1).

<sup>50</sup> CLARA-ANN GORDON, “The Impact of GDPR on International Arbitration – a Practical Guideline”, in *Dispute Resolution Journal*, Volume 74, Issue 4, 2019, pp. 27-34(29). As a consequence, arbitrators should be subjected to the duties consecrated on the GDPR.

<sup>51</sup> On this matter, it is important to point out that Information Commissioner’s Office has really interesting documents in respect to data protection.

<sup>52</sup> NEVA CIRKVENI / PER NEUBURGER, cit. Also stating this is JIE JEANNE HUANG, cit., p. 1208.

<sup>53</sup> Permanent Court of Arbitration (PCA), *Elliott Associates, L.P. (USA) v. Republic of Korea*, No. 2018-51.

<sup>54</sup> Permanent Court of Arbitration (PCA), *Elliott Associates, L.P. (USA) v. Republic of Korea*, No. 2018-51, paragraphs 23-24.

<sup>55</sup> *Ibid*, paragraph 38.

## 2.2. Territorial Scope of the GDPR

Under article 3, it is established the territorial scope of the GDPR.<sup>56</sup> Therefore, the regulation will be applicable when:

(I) In the context of activities of an establishment of a controller or a processor in the Union, regardless whether the processing takes place in the union or not (article 3(1)).<sup>57</sup> Some situations might be considered from this perspective. Clearly, when we think about courts established within the EU, there will be no doubts on the applicability of the diploma. Let's think, for example, about the Vienna International Arbitral Centre ("VIAC"). It will also be possible to establish jurisdiction over the establishment criterion whereas an arbitrator exercises its regular practice within EU.<sup>58</sup> Additionally, Jie Jeanne Huang and Dan Xie raise an important question<sup>59</sup>: what happens to those cases where only one of the parties is from the EU? The authors give as an example the Energy Charter Treaty ("EGT")<sup>60</sup>, as it will be highly likely that at least one of the parties are bound to the GDPR. Having this in mind, and being combined articles 2 and 3, if one of the parties is established in the EU, then the GDPR should be applicable to that particular case.

(II) The GDPR will be applicable even when the controller or processor are not established in the EU, if the processing activities are related to the offering of goods or services,<sup>61</sup> irrespective of whether a payment of the data subject is required, to such data subjects in the union or there is the monitoring of their behavior as far as their behavior takes place within the EU.<sup>62</sup> <sup>63</sup> From what we can see, the "GDPR has a broad application."<sup>64</sup> Having in mind the intention of a global reach, it is necessary to reflect on the several possibilities of applying the GDPR even when the arbitration occurs outside the EU. On the basis of article 3(2)(a), Martin Zahariev states that a situation that might fall within the scope of this provision is the one

<sup>56</sup> Which has as goal, as it is clarified by GRAÇA CANTO MONIZ, cit., p. 49 to protect in an effective way the of the data subject and, on the other hand, allow for the opening of the internal market to any service providers outside the Union, in a way to ensure equity for all companies outside the EU.

<sup>57</sup> See EUROPEAN DATA PROTECTION BOARD, *Guidelines 3/2018 on the territorial scope of the GDPR*, adopted on 16<sup>th</sup> November 2018, pp. 4-12 for an analysis of the criteria mentioned by this provision AND A. BARRETO MENEZES CORDEIRO, "Artigo 3.º", in A. BARRETO MENEZES CORDEIRO (Coord.) *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Coimbra, Almedina, 2021, pp. 70-77(71). See also DAN SVANTESSON, "Article 3. Territorial Scope", in CHRISTOPHER KUNER / LEE A. BYGRAVE / CHRISTOPHER DOCKSEY (ed), *The EU General Data Protection Regulation (GDPR)*, Oxford, Oxford University Press, 2020, pp. 74-99(75).

<sup>58</sup> As MARTIN ZAHARIEV, cit., p. 9 prescribes.

<sup>59</sup> JIE JEANNE HUANG / DAN XIE, cit., p. 16.

<sup>60</sup> As we know the EU and Euratom are parties to the ECT. For an analysis of the EU's proposal for the modernization of the Energy Charter Treaty see MARTA VICENTE, "The European Union's Proposal for the Modernization of the Energy Charter Treaty", in *European Energy and Environmental Law Review*, Volume 31, Issue 3, 2022, pp. 124-134(124).

<sup>61</sup> Article 3(2)(a) of the GDPR. As A. BARRETO MENEZES CORDEIRO, *Direito da proteção de dados...* cit., p. 96 reminds that this applicability outsider the territory of the EU might be difficult for a number of reasons and one of the main issues is, precisely, related to the fact that the GDPR aims to be enforceable outside the EU's borders.

<sup>62</sup> Article 3(2)(b) of the GDPR. EUROPEAN DATA PROTECTION BOARD, *Guidelines 3/2018 cit.*, pp. 12-23.

<sup>63</sup> Thus, it is established the market principle. MANUEL KLAR, "Art. 3 Raumlicher Anwendungsbereich", in JÜRGEN KÜHLING / BENEDIKT BUCHNER (ed), *Datenschutz-Grundverordnung/BDSG Kommentar*, 2.<sup>a</sup> Auflage, Munich, C.H. Beck, 2018, pp. 109-137(113) outlines that this allows it allows "the law of the place to be applied where there is a final intervention in the market and where the data is accessed." (our translation).

<sup>64</sup> ORESTE POLLICINO / MARCO BASSINI / GIOVANNI DE GREGORIO, *Internet Law and the Protection of Fundamental Rights*, Bocconi, Bocconi University Press, 2022, p. 197. As DENIS KELLEHER / KAREN MURRAY, *EU Data Protection Law*, London, Bloomsbury Professional, 2018, p. 112 prescribe "the GDPR takes a bifurcated approach to jurisdiction", not only because on article 3º it seems that it aims for a global jurisdiction and, on the other hand, chapter V establishes several mechanisms to control the transfer of data outside the EU."

where an arbitral institution located in a third-country maintains on its website the tariff for the provision of arbitration services or a calculator for estimating the arbitration costs in United States Dollar and Euros.<sup>65</sup> In fact, in order to determine whether a controller/processor is offering goods or services, it won't be enough that there is a mere accessibility of a website in the EU. On this matter, Recital 23 mentions that the use of language or the currency used in one of more member states is another factor.<sup>66</sup> From an abstract point of view, this could be a feasible option. Nevertheless, it is still difficult to see the GDPR being applicable on this situation to international arbitrations.

This will further depend on a case-by-case analysis, but one thing is certain: even if the GDPR is not applicable to a certain arbitration, we will have to take into consideration the possibility of occurring international data transfers and, therefore, the GDPR might still be considered.

### 2.3. Transfers of Personal Data to third countries

From an international arbitration's perspective, it is also quite important to take into consideration the problem of transfers of personal data to third countries, as "inconsistencies among the data-sharing regimes of foreign countries frustrate the efficient exchange of personal data."<sup>67</sup> On this matter, Elena Mazetova inclusively states that an analysis of the cross-border data transfer and identification of those who should be applicable to a certain case has to be the first step<sup>68</sup>, in order to "provide the parties with clear guidance concerning the applicable rules and potential risks."<sup>69</sup> Hence, a transfer of personal data outside of the EU<sup>70</sup> can be justifiable on the basis of four different grounds, namely:

(I) There is an adequacy decision<sup>71</sup>, which correspond to formal decisions adopted by the Commission declaring that a third country, a territory or one or more specified sectors within that third country, or the international organization in question ensure an adequate level of protection.<sup>72</sup> This is really important, as if there is an adequacy decision, then, no further authorization will be required in order for the transfer to take place. At the moment, the European Commission has recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, New Zealand, Republic of Korea,

<sup>65</sup> MARTIN ZAHARIEV, cit., p. 10.

<sup>66</sup> Inside the EU, most countries have as its official coin Euro.

<sup>67</sup> KIMBERLY A. HOUSER / JOHN W. BAGBY, "The Data Trust Solution to Data Sharing Problems", *Vanderbilt Journal of Entertainment & Technology Law*, Volume 25, Issue 1, 2023, pp. 113-180(128).

<sup>68</sup> ICCA-IBA, *Joint Task Force on Data Protection* cit., p. 17 outlines that this is "one of the most obvious ways that data protection laws apply to international arbitrations."

<sup>69</sup> ELENA MAZETOVA, cit., p. 28.

<sup>70</sup> DAVID M. HOWARD, "Foreign Data Protection in International Arbitration and United States Litigation", in *Texas International Law Journal*, Volume 55, Issue 3, pp. 395-407 makes an interesting comparison and analyzes of this problem under the US's litigation system.

<sup>71</sup> See Article 45 of the GDPR.

<sup>72</sup> The elements foreseen on article 45(2) of the GDPR must be taken into consideration. As CHRISTOPHER KUNER, "Article 45. Transfers on the basis of an adequacy decision", in CHRISTOPHER KUNER / LEE A. BYGRAVE / CHRISTOPHER DOCKSEY (ed) *The EU General Data Protection Regulation (GDPR)*, Oxford, Oxford University Press, 2020, pp. 771-796(777) points out "whether an adequacy decision or an international agreement is used as a legal basis for data transfers depends on a variety of factors, both legal and political."

Switzerland, the UK and Uruguay as providing adequate protection. On the other hand, this is not permanent, as there is a constant obligation to monitor developments in third countries and international organizations that could affect the functioning of decisions adopted.<sup>73</sup> However, transposing this to the arbitration framework “may be difficult (if not impossible) to create an environment fully covered by adequacy decisions”.<sup>74</sup> Thus, within the context of international arbitration, most of the transfers normally happen to countries that don’t have an adequacy decision. Let’s think on the example of the Singapore, Hong Kong, India, Australia, among others, which are really important countries in terms of arbitration.<sup>75</sup> Recently, the European Commission adopted its adequacy decision for the EU-US Data Privacy Framework, but we will still have to see its impact and, above all, the ECJ’s reaction towards it.<sup>76</sup> Still, having in mind the limited scope for these decisions, in regards to international arbitration, most times it will not be very helpful.

(II) Another possibility is using article 46 of the GDPR, which foresees the possibility of transferring personal data to a third country or an international organization if the controller or processor has provided appropriate safeguards.<sup>77</sup> Related to this, article 46(2) foresees some examples of what might be considered an appropriate safeguard. ICCA-IBA Report outlines that the most adequate is the standard contractual clauses and, on Annex 6, it gives a sample standard of how this should be addressed.<sup>78</sup> However, as David Rosenthal prescribes, this might be tricky in regards to arbitration, due to the fact that these standard clauses have to be used with no changes<sup>79</sup> and some parties might have not signed the clauses, as they may lead to the increase of the liabilities.<sup>80</sup> Even though safeguards are the preferable option (before trying to apply article 49), within the context of litigation, this may not be feasible.<sup>81</sup>

(III) Additionally, article 49 is another alternative for international transfers. When applying this article, the “data exporter transferring personal data to third countries or international organizations must also meet the conditions of the other provisions of the GDPR.”<sup>82</sup> Article 49 is also seen as a last resource, as data exporters should first explore possibilities to frame the

<sup>73</sup> It is called periodic review. See Article 45(4) of the GDPR. See also ALEXANDRE DE SOUSA PINHEIRO / CARLOS JORGE GONÇALVES, “Artigo 45.º Transferências com base numa decisão de adequação”, ALEXANDRE SOUSA PINHEIRO et. al. (ed) *Comentário ao Regulamento Geral de Proteção de Dados*, Coimbra, Almedina, 2018, pp. 504-512(504), CHRISTOPHER KUNER, cit., pp. 790-791, GRAÇA CANTO MONIZ, cit., pp. 288-290.

<sup>74</sup> ELENA MAZETOVA, cit., p. 30.

<sup>75</sup> DAVID ROSENTHAL, cit., p. 829.

<sup>76</sup> In fact, the Commission has tried to adopt a decision of adequacy to the USA for a long time. The ECJ invalidated the decision, due to the fact that the provisions didn’t provide an adequate protection to data subjects in the EU. We’re not going to analyze the Saga Schrems here, but it is necessary to outline the importance of this jurisprudence. See European Court of Justice (ECJ), Maximilian Schrems v. Data Protection Commissioner (Schrems I), 6/10/2015 C-362/14; European Court of Justice (ECJ), Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems (Schrems II), C-311/18, 16/07/2020 (this was the one where the ECJ invalidated the EU-US Privacy Shield. *Vide* ORESTE POLLICINO / MARCO BASSINI / GIOVANNI DE GREGORIO, cit., pp. 239-250.

<sup>77</sup> See ORESTE POLLICINO / MARCO BASSINI / GIOVANNI DE GREGORIO, cit., pp. 236-238. Graça Canto Moniz, cit., pp. 290-294.

<sup>78</sup> ICCA-IBA, *supra* note 11, 90-117.

<sup>79</sup> DAVID ROSENTHAL, cit., p. 8.

29-830.

<sup>80</sup> As DAVID M. HOWARD, cit., p. 399, recalls.

<sup>81</sup> KATHLEEN PAISLEY, cit., p. 879.

<sup>82</sup> EUROPEAN DATA PROTECTION BOARD, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, adopted on 25<sup>th</sup> May 2018, p. 3.

transfer within other mechanisms included in articles 45 and 46(1) of the GDPR.<sup>83</sup> For this reason, the European Data Protection Board clarifies that such transfers may happen more than once, but they cannot be considered regular.<sup>84</sup> By analyzing the different possibilities, we believe that the most adequate is article 49(1)(e), under which the transfer of personal data will be possible whenever it is necessary for the establishment, exercise or defense of a legal claim.<sup>85</sup> The European Data Protection Board defends a broad interpretation, as it considers that many activities can be included (for example: criminal or administrative investigation in a third country, data transfers for the purpose of formal pre-trial discovery procedures or anti-trust investigations).<sup>86</sup> However, it is clarified that this does not include the mere possibility of those legal proceedings being brought in the future.<sup>87</sup> Arbitration is a form of resolving disputes that offer involved parties an alternative to classic litigation, which has its own formal and legal proceedings. As a consequence, article 49(1)(e) has to be considered a feasible option. This position is also shared by David Rosenthal.<sup>88</sup> In addition, Elena Mazetova also states that within the context of arbitration, the transfer of personal data will occur “on an ad hoc basis.”<sup>89</sup> It is a requirement, if this basis is invoked, that the transfer is necessary<sup>90</sup>, occasional<sup>91</sup>, being also mandatory that the personal data subject to it is minimized to what is strictly essential.<sup>92</sup>

Thus, David Rosenthal proposes that an agreement could be made between the parties, the counsel and the arbitrators, in order to clarify that “each party should only submit personal data that is necessary for the proceedings, to keep such personal data confidential, and use it only for the arbitration and related purposes.”<sup>93</sup> Hence, the Author further points out that everyone should sign it, regardless of the level of data protection in the country.<sup>94</sup> Moreover, and regardless any considerations on this point, we think that Elena Mazetova has a point when the author argues that assessing the necessity test is not always easy when we think about arbitration. In fact, if a party requests a certain document, then it will be easy to assess if that request will be helpful and meet the criteria defined under the GDPR. Moreover, if it is

<sup>83</sup> Ibid, p. 4.

<sup>84</sup> EUROPEAN DATA PROTECTION BOARD, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679* cit., p. 4. *Vide* Recital 111.

<sup>85</sup> This provision must be read in conjunction with Recital 111 of the GDPR, which among other things provides that the transfer can be made “occasional and necessary in relation to a contract or a legal claim regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies.” *Vide* ALEXANDER BLUMROSEN, cit., p. 102.

<sup>86</sup> EUROPEAN DATA PROTECTION BOARD, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, cit., p. 11.

<sup>87</sup> EUROPEAN DATA PROTECTION BOARD, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, cit., p. 18 if the transfer is occasional in relation to that legal proceeding, then this won’t serve as a basis for the transfer. See ALEXANDRE SOUSA PINHEIRO / CARLOS JORGE GONÇALVES, “Artigo 49.º Derrogações para situações específicas”, in ALEXANDRE SOUSA PINHEIRO et. al. (ed) *Comentário ao Regulamento Geral de Proteção de Dados*, Coimbra, Almedina, 2018, pp. 524-530(528).

<sup>88</sup> DAVID ROSENTHAL, cit., p. 830. DAVID M. HOWARD, cit., pp. 398-400.

<sup>89</sup> ELENA MAZETOVA, cit., p. 34.

<sup>90</sup> As the EUROPEAN DATA PROTECTION BOARD, *Guidelines 3/2021 on the territorial scope of the GDPR (Article 3)*, adopted on 7th January 2020, p. 12 outlines, the necessity test will require a close and substantial connection between the data and the specific establishment, exercise or defense of the legal position. Therefore, “the mere interest of third country authorities” is not sufficient.

<sup>91</sup> Ibid, p. 4.

<sup>92</sup> See also ICCA-IBA, *Joint Task Force on Data Protection* cit., p. 18.

<sup>93</sup> DAVID ROSENTHAL, cit., p. 830. Also proposing agreements among parties when it is possible, see KATHLEEN PAISLEY, cit., p. 881.

<sup>94</sup> DAVID ROSENTHAL, cit., pp. 830-831.

something introduced in a memorandum or other document voluntarily introduced, as the author prescribes, a more detailed explanation will be needed.<sup>95</sup>

Finally, as a last resource, a mention should be made to article 49(1)§2 of the GDPR, which provides that, even if none of the derogations foreseen on article 49(1) are applicable, the transfer might occur if (i) concerns only a limited number of data subjects, (ii) is necessary for the purposes of compelling legitimate interests and (iii) the controller has assessed all the circumstances surrounding the data transfer and has provided for suitable safeguards. Additionally, the supervisory authority of the transfer shall be informed, as well as the data subjects. Even if, from an abstract point of view, it might be applicable, due to the strict requirements, we do not see as this could be a suitable mean for the different parties.<sup>96</sup>

As the doctrine identifies, it seems that the best option for international transfers within the context of international arbitration, will be article 49(1)(e) of the GDPR. What this represents is that, even if the material and territorial requirement is not met, the GDPR may still apply, even if incidentally, to arbitrations being held outside the EU.

### 3. Specific issues regarding the Arbitral Proceeding

#### 3.1. Online Hearings

Hearings are a very important step within the context of international arbitration, as a proceeding won't probably end without one occurring.<sup>97</sup> With COVID'19, it became normal to hold these hearings online, due to the requirements of non-personal contact. This has several advantages, as it allows to reduce costs<sup>98</sup> and increase efficiency.<sup>99</sup> Thus, these advantages can be also seen from a different perspective, due to the problems that arise. Firstly, it creates a higher risk for cyberattacks<sup>100</sup>, as well as it might be problematic from a data protection point of view (we'll have the change to analyze the challenges on regards to the GDPR later)

<sup>95</sup> ELENA MAZETOVA, cit., p. 39.

<sup>96</sup> ICCA-IBA, *Joint Task Force on Data Protection* cit., p.18.

<sup>97</sup> As NIGEL BLACKABY et. al., *Redfern and Hunter on International Arbitration*, Oxford, Oxford University Press, 2015, p. 400 reminds. PILAR PERALES VISCASILLAS, "An Arbitrator's Perspective: Online hearings in Arbitration: the taking of Evidence", in DÁRIO MOURA VICENTE / ELSA DIAS OLIVEIRA / JOÃO GOMES DE ALMEIDA (ed) *Online Dispute Resolution New Challenges*, Baden-Baden, Nomos, 2022, pp. 107-131(109) considers that the pandemic demonstrated the "adaptability of international commercial arbitration to the needs of the arbitration industry, and its capacity for innovation."

<sup>98</sup> In fact, it might be arguable that "oral hearings are the most cost-intensive periods of any arbitration", as a lot of mechanisms must be ensured in order for it to happen (NIGEL BLACKABY et. al, cit., p. 401). We're thinking not only about the perspective of the parties (who, most likely, will have to travel in order to attend those hearings, as well as the tribunal itself). Additionally, as MADALENA DINIS DE AYALA, "The Rising Inefficiency in Arbitration: is Technology the Solution?", in *Revista de International de Arbitragem e Conciliação*, Volume XVI, 2021, pp. 115-145(130) mentions "witness travel, accommodation, preparation, document production, and above all, the location of hearings, massively contribute to increase arbitration costs." If conducted online, then, these costs will be significantly reduced.

<sup>99</sup> BELEN OLMOS GIUPPONI, "Virtual Dispute Resolution in International Arbitration – Mapping its advantages and main caveats in the Face of Covid-19", in SHAHEEZA LALANI / STEVEN G. SHAPRIO (ED) *The Impact of Covid on International Disputes*, Leiden, Brill Nijhoff, 2022, pp. 62-83(71).

<sup>100</sup> For example, in 2015, the website of the PCA was hacked while there was an ongoing maritime border dispute between China and the Philippines.

and may emerge problems related to confidentiality.<sup>101</sup> After all, as some doctrine outlines, “there is no longer any question of if one’s digital infrastructure and data will be hacked, but only when.”<sup>102</sup> Additionally, issues might be raised relating to the authenticity of the hearing itself, as a personal contact might be better (at least for some) to assess the authenticity of what is being said.<sup>103</sup>

Despite these factors, it is important to point out that this is a matter to which a significant importance is given. Nevertheless, the answer to the question to know if the hearing can happen online, “entails a case-by-case analysis.”<sup>104</sup> In fact, article 28(4) of UNCITRAL Arbitration Rules<sup>105</sup> foresees that “the arbitral tribunal may direct that witnesses (...) are examined through means of telecommunication that do not require their physical presence at the hearing.” A similar provision might be found on article 24(4) of International Chamber of Commerce (“ICC”) Rules of Arbitration<sup>106</sup>, article 19(2) of The London Court of International Arbitration Rules (“LCIA”)<sup>107</sup> or article 30(1) of VIAC Rules.<sup>108</sup>

Arbitration operators and arbitration institutions, as Pilar Perales Viscasillas states, “were catalysts for this process of adaptation, even before the Covid, especially in matters related to the security of new technologies.”<sup>109</sup> Besides, several reports have been adopted on this matter, which corroborates the fact that this is an important topic for arbitration.<sup>110</sup>

As we already know, these online hearings will lead to the processing of personal data. Therefore, if it is a situation that falls within the scope of the GDPR, then some additional steps must be taken into account in order to fulfill its demands. It will depend on the case-by-case

<sup>101</sup> BELEN OLMOS GIUPPONI, cit., p. 72. After all, as BAHAR HATAMI ALAMDARI, “The Question of Remote Hearings in International Commercial Arbitration”, in SHAHEEZA LALANI / STEVEN G. SHAPIRO (ed), *The Impact of Covid on International Disputes*, Leiden, Brill Nijhoff, 2022, pp. 141-156(154) who reminds that, due to the characterization of arbitration as a confidentiality proceeding, that the reason why many times the parties choose it.

<sup>102</sup> STEPHANIE COHEN / MARK MORRIL, “A Call to Cyberarms: The International Arbitrator’s duty to avoid digital intrusion”, in *Fordham International Law Journal*, Volume 40, Issue 3, pp. 981-1022(1009).

<sup>103</sup> Having this in mind, as PILAR PERALES VISCASILLAS, cit., p. 123 points out, an online hearing might implicate more preparation by lawyers, in order to define the questions and set the interrogation and cross-examination. There might be another inconvenient for the parties, which is related to the different time zones of participants. This might make it harder to conciliate different agendas. *Vide* BAHAR HATAMI ALAMDARI, cit., p. 154. See also MADALENA DINIS DE AYALA, cit., p. 131. As the author outlines, online hearings are impersonal and, therefore, it is not possible to replicate the “formality of the arbitration process”, which leads to the disappearance of “its main essence.”

<sup>104</sup> BELEN OLMOS GIUPPONI, cit., p. 66.

<sup>105</sup> United Nations Commission on International Trade Law, UNCITRAL Rules and Model Law Arbitration Rules.

<sup>106</sup> ICC Rules of Arbitration which entered into force on 1 January 2021. It foresees that “case management conferences may be conducted through a meeting in person, by video conference, telephone or similar means of communication.” In the absence of an agreement between the parties, the arbitral tribunal shall determine the means by which the conference will be conducted.

<sup>107</sup> Article 19(2) of London Court International Arbitration Rules provides that “As to form, a hearing may take place in person, or virtually by conference call, videoconference or using other communications technology with participants in one or more geographical places (or in combined form).”

<sup>108</sup> Article 30(1) of VIAC Rules provides that “having due regard to the views of the parties and the specific circumstances of the case, the arbitral tribunal may decide to hold an oral hearing in person or by other means.”

<sup>109</sup> PILAR PERALES VISCASILLAS, cit., p. 112.

<sup>110</sup> The KOREAN COMMERCIAL ARBITRATION BOARD (“KCAB”), *Seoul Protocol on Video Conferencing in International Arbitration*, adopted on 18<sup>th</sup> March 2020. ICCA-IBA, *Joint Task Force on Data Protection* cit., pp. 62-63, which also addresses the topic of remote hearings, by pointing out the most important aspects HONG KONG INTERNATIONAL ARBITRATION CENTER (“HKIAC”), *Guidelines for Virtual Hearings*, adopted on 15<sup>th</sup> May 2020, available <https://www.hkiac.org/news/hkiac-guidelines-virtual-hearings> (02.12.2023). Furthermore, the AMERICAN ARBITRATION ASSOCIATION (“AAA”) and THE INTERNATIONAL CENTRE FOR DISPUTE RESOLUTION (“ICDR”) have adopted something similar. See AAA-ICDR, *Virtual Hearing Guide For Arbitrators and Parties*, adopted on 9<sup>th</sup> May 2020. These are just some of the many examples that may be pointed out, but several more could be taken into account.

analysis to know who might in the specific case be considered the controller<sup>111</sup> or a processor<sup>112</sup>, being possible to also exist a joint controllership.<sup>113</sup> Moreover, and regardless of deeper considerations on this matter<sup>114</sup>, obligations arise due to the application of the GDPR in the arbitration.

Firstly, during these online hearings, it results from article 32 of the GDPR an obligation to ensure security of processing. This is a previous obligation, as Maria da Graça Moniz outlines<sup>115</sup>, which means that the responsible entities for the processing shall implement appropriate, technical and organizational measures to increase the level of security. In fact, some doctrine argues that Recital 81 of the GDPR should be seen as a new “criterion for the choice of arbitrators and arbitral institutions.”<sup>116</sup> On this matter, the ICCA-BY Bar-CPR Protocol on Cybersecurity has as principle, among other things, the determination of reasonable cybersecurity measures<sup>117</sup>.

Even though this has been thought from a cybersecurity perspective, we shall not ignore that under the GDPR this is very important.<sup>118</sup> Therefore, the regulation gives some examples of what might lead to the increase of security system, namely: pseudonymization and encryption of personal data<sup>119</sup>, ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services<sup>120</sup>, restore availability and access to personal data in a timely manner in the event of a physical or technical incident<sup>121</sup>, create a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.<sup>122</sup>

On this matter, Marc Henry advocates that the best way during an international proceeding to fulfill this intention is the use of platforms, because that might, in his opinion, “level up the overall security of the custody chain as long as the relevant functions are enable and used.”<sup>123</sup> However, it will depend on the type of platform, because it is necessary to ensure its safety.<sup>124</sup> After all, this will mean that “the infrastructure used by the Arbitral Participants to secure the

<sup>111</sup> According to article 4(7) of the GDPR controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

<sup>112</sup> According to article 4(8) of the GDPR means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

<sup>113</sup> Which happens where two or more controllers jointly determine the purposes and means of processing; they shall be joint controllers – article 26(1) of the GDPR. Vide KATHLEEN PAISLEY, cit., p. 867.

<sup>114</sup> KATHLEEN PAISLEY, cit., pp. 893-899. NICCOLÒ LANDI, “Remote Hearings: Observations on the Problem of Personal Data Protection and Cybersecurity”, in *Does a Right to a Physical Hearing Exist in International Arbitration? International Council for Commercial Arbitration*, 2022, pp. 127-165, available <http://www.arbitration-icca.org/> (12.12.2023).

<sup>115</sup> GRAÇA CANTO MONIZ, cit., p. 242-243.

<sup>116</sup> NICCOLÒ LANDI, cit., p. 156.

<sup>117</sup> ICCA-NYC Bar-CPR, *Protocolo on Cybersecurity* cit., p. 15.

<sup>118</sup> On this matter, NEVA CIRKVENI / PER NEUBURGER, cit., state that the different reports on this matter don’t address specifically the issues that might be raised from a GDPR perspective.

<sup>119</sup> Article 32(1)(a) of the GDPR.

<sup>120</sup> Article 32(1)(b) of the GDPR.

<sup>121</sup> Article 32(1)(c) of the GDPR.

<sup>122</sup> Article 32(1)(d) of the GDPR.

<sup>123</sup> MARC HENRY, “An Arbitrator’s Perspective: Confidentiality – Privacy – Security in the Eye of the Arbitrators or the Story of the Arbitrator who Became a Bee”, in Dário Moura VICENTE, / ELSA DIAS OLIVEIRA / JOÃO GOMES DE ALMEIDA, (ed) *Online Dispute Resolution – New Challenges*, Baden-Baden, Nomos, 2022, pp. 181-204(183).

<sup>124</sup> EMILY HAY, cit., states that certification of technical standards (such as ISO/IEC27001) are desired.



arbitration ought to be state of the art.”<sup>125</sup> Thus, it is up to the Tribunals to play a crucial role when assessing and choosing the tool for video conferencing. ICCA-IBA’s Joint Task Force points out that the tribunal must consult with the parties to establish a remote hearing protocol to address issues like (i) the technology used, (ii) advanced testing of the technology or training, (iii) starting and ending times, having in mind the different time zones, (iv) how documents will be placed before a witness and (v) measures to ensure that witnesses giving testimony are not distracted or improperly.<sup>126</sup> Additionally, Emily Hay outlines the importance, as article 32(1)(b) of the GDPR demands, of ensuring that the video transmissions have end-to-end encryption.<sup>127</sup>

On a further note, special emphasis should be made to the legal basis of processing. Under article 6 of the GDPR, processing shall be lawful only if it is possible to invoke one of the following legal basis: consent, contract, legal obligation, vital interests, public task or legitimate interests.

Under article 4(11) of the GDPR, consent is lawful whenever it is freely given,<sup>128</sup> specific,<sup>129</sup> informed<sup>130</sup> and unambiguous.<sup>131</sup> One must carefully assess whether consent can be seen as a good legal basis for the arbitration’s context, especially for online hearings. In abstract, we could argue that, before the online hearing, the data subject could freely give its consent for the processing of personal data. Regarding litigation, Article 29 Data Protection Working Party has outlined that there may be situations where individuals are aware of, or even involved in the litigation process, and consent may properly be relied upon as a ground for processing.<sup>132</sup> Nevertheless, Article 29 Data Protection Working Party has also clarified that relying on consent may prove to “be a false good solution, simple at first glance but in reality complex and cumbersome.”<sup>133</sup>

From our point of view, there are two difficulties that may lead to the impracticality of invoking this legal basis in regards to online hearings. On a first note, the data subject may withdraw

<sup>125</sup> ANANYA BAJPAI / SHAMBHAVI KALA, *cit.*, p. 13.

<sup>126</sup> ICCA-IBA, *Joint Task Force on Data Protection* *cit.*, p. 63.

<sup>127</sup> EMILY HAY, *cit.*

<sup>128</sup> Freely given means that the consent must imply a real choice and control for data subjects. Consent cannot be considered freely given whenever there is an imbalance of power between the controller and the data subject (which will be the case for public authorities – Recital 43). Additionally, under article 7(4) of the GDPR, when assessing whether is freely given, utmost account shall be taken of whether the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract (conditionality). As the EUROPEAN DATA PROTECTION BOARD, *Guidelines 05/2020 on consent under Regulation 2016/679*, Version 1.1, adopted on 4th May 2020, p. 10, recalls, “Compulsion to agree with the use of personal data additional to what is strictly necessary limits data subject’s choices and stands in the way of free consent.” Furthermore, whenever a service involves multiple processing operations for more than one purpose, the data subjects have to be given the possibility to choose which purposes they accept (granularity). Finally, for the consent to be considered freely given, the controller will need to demonstrate that it is possible to refuse or withdraw consent without detriment (recital 42).

<sup>129</sup> The consent of the data subject must be given in relation to one or more specific purposes. This aims to a certain level of transparency and control.

<sup>130</sup> As the EUROPEAN DATA PROTECTION BOARD, *Guidelines 05/2020 on consent under Regulation 2016/679*, *cit.*, p. 15 outlines “providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example, exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and consent will be an invalid basis for processing.”

<sup>131</sup> It requires, as a consequence, either a statement or a clear affirmative act.

<sup>132</sup> ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working Document 1/2009 on pre-trial discovery for cross border civil litigation*, adopted on 11th February 2009, p. 9.

<sup>133</sup> *Ibid*, p. 9.

its consent at any time<sup>134</sup>, which means that this will “present a challenge where arbitration proceedings been initiated.”<sup>135</sup> Therefore, this could endanger the proceeding itself, as at any time the data subject would maintain the possibility to revoke its consent for the processing of personal data. Even though that is applicable to the future, it does not seem easy to prevent the effects on the arbitration’s proceeding, especially when the online hearing constitutes a crucial element of proof.<sup>136</sup>

Additionally, we must also take into consideration that invoking consent would be impractical due to the complexity of the proceeding<sup>137</sup>, as in each case it would be necessary to demonstrate that the data subject participating in the online hearing had given its consent for that act. This would create more unnecessary bureaucracy, when there may be more suitable options to invoke as a legal basis. The ICCA-IBA’s Roadmap to Data Protection in International Arbitration adopts the same position, as it clarifies that the Arbitral Participant is the one providing the personal data, “including each data subject identified or identifiable from the submissions or evidence”.<sup>138</sup> This level of uncertainty is not desired for arbitrators and the parties.

For online hearings, this does not constitute, in our line of thought, the legal basis. The use of consent must be accompanied by a meticulous evaluation of its practicability in the specific context. As a consequence, one suitable legal basis might be the legitimate interest, under article 6(1)(f) of the GDPR.<sup>139</sup> This requires a three-step analysis, namely: (i) there is a legitimate interest, (ii) it is necessary and (iii) these interests are not overridden by the interests or fundamental rights and freedoms of data subjects. As David Rosenthal points out, having in mind that arbitration aims to ensure confidentiality and have to adopt specific criterion and determine the different facts, there is a legitimate interest and, by taking into consideration, the two sides, it seems justifiable.<sup>140</sup> One should also bear in mind that “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.”<sup>141</sup> In what concerns online hearings, a step-by-step analysis must be considered, in order to evaluate the type of platform used, how the data is collected and which preventive measures can be adopted in order to balance this situation.

Additionally, even if relying on this type of legal basis, the data subject still has to be ensured the different rights conferred by the GDPR. Therefore, the importance of the right to

---

<sup>134</sup> Article 7(4) of the GDPR.

<sup>135</sup> MO EGAN / HONG-LIN YU, “Intersecting and Dissecting Confidentiality and Data Protection in Online Arbitration”, *Journal of Business Law* (forthcoming), 2022, pp. 1-27(13), available at <https://dspace.stir.ac.uk/handle/1893/31758> (29.04.2024).

<sup>136</sup> KATHLEEN PAISLEY, cit., pp. 874-875. MO EGAN / HONG-LIN YU, cit., p. 13.

<sup>137</sup> Even for a witness statement, as DAVID ROSENTHAL, cit., p. 834 recalls. See, also, NICCOLÒ LANDI, cit., p. 148 and GEORGE A. BERMANN, cit., p. 155.

<sup>138</sup> INTERNATIONAL COUNCIL FOR COMMERCIAL ARBITRATION (ICCA) / INTERNATIONAL BAR ASSOCIATION (IBA), *Joint Task Force on Data Protection in International Arbitration – Roadmap to Data Protection in International Arbitration* cit., p. 43.

<sup>139</sup> Vide GRAÇA CANTO MONIZ, cit., pp. 91-99.

<sup>140</sup> DAVID ROSENTHAL, cit., p. 834

<sup>141</sup> KATHLEEN PAISLEY, cit., p. 876.

information cannot be ignored. During the initial communications with the parties,<sup>142</sup> the necessary information shall be provided, in order to fulfill what is consecrated on articles 13 and 14 of the GDPR.<sup>143</sup>

There is, as Niccolò Landi points out “a general duty to avoid unauthorized interference by third parties.”<sup>144</sup> A breach of security might undermine not only the process itself, as well as leading to the liability under Chapter VIII of the GDPR, whose fines might achieve significant values.<sup>145</sup> For this reason, despite the responsibilities that might result from the applicability of the GDPR, some doctrines argues that from an arbitration’s perspective, the arbitrators’ duty to an obligation to take these measures should be limited whenever he/she “deems reasonable in light of the relevant facts and circumstances.”<sup>146</sup> Marc Henry sums it all:

“[O]nce the data (just like pollen) is brought into the arbitral hives, the data needs to be protected from external predators. In the same way that soldier bees protect the hives from external attacks, arbitrators will assume the role of soldiers in the fight against cyber-attacks, and therefore contribute to the security of the arbitral process.”<sup>147</sup>

### 3.2. Evidence

One question that also might arise is related to the disclosure of evidence, namely to know if a party can refuse giving it on the basis of the GDPR. Evidence assumes a crucial role in International Arbitration, as each party will aim to provide to the arbitral tribunal the most coherent material in order to prove its assertions. Each party, due to its autonomy, will have to carry out a careful assessment of the evidence delivered to the tribunal. It is not, therefore, enough to affirm a fact, as everything has to be proven.

As Tanmayi Sharma recalls, “the general practice of arbitral tribunals is that the weight of evidence is assessed depending on the nature of the proposition it seeks to prove.”<sup>148</sup> Hence, ICCA and IBA also recognize this as one of the key aspects during the arbitration.<sup>149</sup>

We should point out that this is not a mere academic problem, as it might raise important problems, not only regarding the GDPR (and other data protection’s regulations), as well as cybersecurity. For example, in *ConocoPhillips v. Venezuela*<sup>150</sup>, after issuing the award, the tribunal had to deal with new facts, as Venezuela sent a letter to the Tribunal contesting the

<sup>142</sup> EMILY HAY, cit.

<sup>143</sup> Article 13 relates to information that has to be provided where personal data is collected from the data subject. Article 14 relates to information to be provided where personal data have not been obtained from the data subject.

<sup>144</sup> NICCOLÒ LANDI, cit., p. 159. STEPHANIE COHEN / MARK MORRIL, cit., p. 1009.

<sup>145</sup> See Articles 83 and 84 of the GDPR. These different actors, as MARC HENRY, cit., p. 197, prescribes are “no longer only responsible, but they are also accountable.”

<sup>146</sup> STEPHANIE COHEN / MARK MORRIL, cit., p. 1011.

<sup>147</sup> MARC HENRY, cit., p. 197.

<sup>148</sup> TANMAYI SHARMA, “Evidence in International Arbitration: Admissibility, Relevance and Differences between Common and Civil Law”, in *Católica Law Review*, Volume II, n.º 2, 2018, pp. 99-113(103).

<sup>149</sup> ICCA-IBA, *Joint Task Force on Data Protection* cit., p. 57.

<sup>150</sup> International Center for Settlement of Investment Disputes (ICSID), *ConocoPhillips v. Venezuela*, no. ARB/07/30.

decision, by invoking evidence that was obtained via WikiLeaks which demonstrated that communications were made between diplomatic officials in the US’s Embassy and Conoco Phillips’ executives discussing the offer of compensation made the Venezuela Government.

The Tribunal, nevertheless, did not address this issue, as it only pointed out that it did not have the power to reconsider the decision adopted on 3th September 2013.<sup>151</sup> Hence, we are confronted with the issue to know which framework shall be given to these kinds of situations.<sup>152</sup> We should also bear in mind that this might impose issues in regards to the GDPR, as evidence obtained due to a hacker’s attack raises questions from a data protection’s point of view.

We should now enter the main focus of this chapter, namely to know if it is possible for the parties to invoke the breach of the GDPR and refuse certain evidence. First and foremost, a brief look at the different rules demonstrates the importance of it. For example, Article 27(1) of UNCITRAL Arbitration Rules clearly points that each party has the burden of proving the facts relied on to support its claim or defense, adding that any time during the proceedings the tribunal may require the parties to produce documents, exhibits or other evidence.<sup>153</sup> The ICSID Convention also foresees, except if the parties otherwise agree, that the Tribunal may, if it deems necessary at any stage of the proceedings, to call upon the parties to produce documents or other evidence.<sup>154</sup> IBA has also adopted a document based on the Rules on the Taking of Evidence in International Arbitration.<sup>155</sup> Many more could be mentioned, but it would fall outside the scope of this study.

It remains open the question of whether it is possible for a party to refuse the disclosure of a document, for example, on the basis that its processing is prohibited by the GDPR. Nothing can expressly be found on its provisions. Hence, this is interesting, because recently the ECJ has addressed this issue (even if within the context of civil litigation) in case *Norra Stockholm Bygg AB v. Per Nycander AB, Entral AB*.<sup>156</sup> It argued that, when assessing the production of a document containing personal data, the national court has to take into account the interests of the data subjects and balance the different interests depending on the circumstances of each case.<sup>157</sup> Further, the Court defended that, when the production of a document proves to be justified, the national authorities still have to take additional measures of protection, in order to increase the level of protection of the processing for these goals.<sup>158</sup>

<sup>151</sup> International Centre for Settlement of Investment Disputes, *ConocoPhillips v. Venezuela*, ICSID Case no. ARB/07/30, Decision on Respondent’s Request for Reconsideration, 2014, available (19.11.2023).

<sup>152</sup> As PIERRE BIENVENU / BENJAMIN GRANT, “Data Protection and Cyber risk issues in Arbitration”, in *International Arbitration Report*, Issue 13, Norton Rose Fulbright, 2019, pp. 19-21(21) point out “there is little evidence as yet that a consistent approach to dealing with these issues is emerging. As data breaches become more common, tribunals will be called on more frequently to rule on the admissibility of such evidence.”

<sup>153</sup> Article 27(3) UNCITRAL Arbitration Rules.

<sup>154</sup> Article 43(a) ICSID Convention, Regulations and Rules.

<sup>155</sup> IBA, *Rules on the Taking of Evidence in International Arbitration*, adopted on 17th December 2020, available <https://www.ibanet.org/> (02.01.2024).

<sup>156</sup> Court of Justice (CJ) *Norra Stockholm Bygg AB v. Per Nycander AB, Entral AB*, 02/03/2023, C-268/21.

<sup>157</sup> Court of Justice (CJ) *Norra Stockholm Bygg AB v. Per Nycander AB, Entral AB*, 02/03/2023, C-268/21, paragraphs 47-55.

<sup>158</sup> *Ibid*, paragraphs 56-57.

Applying this, *mutatis mutandis*, to International Arbitration, we will also need a case-by-case analysis. We do not think, however, that a party can *per se* refuse the disclosure of a certain document due to the GDPR. As David Rosenthal points out, stakeholders “should not gather evidence under false pretext or in an illegal manner.”<sup>159</sup> After all, it will always depend on the necessity in each case to produce certain evidence.<sup>160</sup>

As we have seen, almost everything during the proceedings will constitute personal data and there will be a processing in accordance to the GDPR. Still, not any document will be justified, being essential that the party only has to disclose what is really necessary for the proceeding. Special attention should be given to the principle of data minimization.<sup>161</sup> This has three essential pillars, namely: adequacy, relevancy and necessity.<sup>162</sup> Therefore, as the ECJ has pointed out, “the national court is required to determine whether the disclosure of personal data is adequate and relevant for the purpose of attaining the objective pursued by the applicable provisions.”<sup>163</sup> On the other hand, as Célie de Terwangne underlines, “it is accordingly clear that one may not process an excessively large amount of personal data.”<sup>164</sup>

Besides, Article 29 Data Protection Working Party in the Guidelines on pre-trial discovery for cross border civil litigation<sup>165</sup> has clarified that each of the different stages in civil litigation process will require an appropriate condition in order to legitimize the processing. We can apply this, *mutatis mutandis*, to the arbitration context. In what concerns documentary evidence, it does not seem suitable making its submission dependent of consent. The different documents may entail personal data of a certain identified or identifiable individual. Therefore, the reasoning made for online hearings can be applicable, *mutatis mutandis*, to this context. Making the tribunal and the parties being dependent in each case of consent would undermine and make the proceeding slower. Consequentially, we may think about invoking, as a legal basis for processing, the legitimate interest, under article 6(1)(f) of the GDPR. Nonetheless, it is important to note that “it is possible for member states to supplement these grounds with specific requirements that must be satisfied.”<sup>166</sup> For this reason, a careful evaluation must be made concerning these different jurisdictions.

We must also reflect about the processing of special categories of personal data.<sup>167</sup> It is possible that a certain piece of documentary evidence implies its processing. As we know,

<sup>159</sup> DAVID ROSENTHAL, cit., pp. pp. 833-834.

<sup>160</sup> See CLARA-ANN GORDON, cit., p. 31.

<sup>161</sup> Foreseen on article 5(1)(c) of the GDPR. EUROPEAN DATA PROTECTION BOARD, *Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default*, adopted on 20<sup>th</sup> October 2020, pp. 21-23.

<sup>162</sup> A. BARRETO MENEZES CORDEIRO, *Direito da proteção de dados...* cit., p. 159. As GRAÇA CANTO MONIZ, cit., pp.114-116 recalls adequacy, alongside with reliance, will demand a rational connection with its purpose of processing.

<sup>163</sup> Court of Justice (CJ) *Norra Stockholm Bygg AB v. Per Nycander AB, Entral AB*, 02/03/2023, C-268/21, paragraph 54.

<sup>164</sup> CÉLIE DE TERWANGNE, “Article 5: Principles Relating to processing of personal data”, in CHRISTOPHER KUNER / LEE A. BYGRAVE / CHRISTOPHER DOCKSEY (ed), *The EU General Data Protection Regulation (GDPR)*, Oxford, Oxford University Press, 2020, pp. 309-320(317).

<sup>165</sup> ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working Document 1/2009 on pre-trial discovery for cross border civil litigation*, cit., p. 7.

<sup>166</sup> MO EGAN / HONG-LIN YU, cit., p. 14.

<sup>167</sup> Processing of personal data revealing 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 shall be prohibited.

under article 9(1) of the GDPR, the processing of sensitive data is generally prohibited, except in the situations foreseen on article 9(2) of the GDPR. It will be crucial that in that case not only one of the legal basis foreseen on article 6 is invoked, as well as one of the exceptions mentioned on article 9(2).

This is not an easy topic. At first sight, we can evaluate the possibility to apply article 9(2)(f), which relates to the processing necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity.<sup>168</sup> However, we must take into consideration that international arbitration has its own specificities when compared to traditional litigation. In addition, it is not well clarified what “necessary” means on this context and, due to the fact that this is not a traditional case of litigation, from a literal point of view, it could be difficult to apply. Nonetheless, from all the options available, it seems the only one that can be invoked.

The Tribunal should ensure all the safety measures when sensitive data is included on the documentary evidence, in order to balance these different interests: not only the ones regarding the proceeding itself (namely, matters of confidentiality), as well as the data subject’s rights. This will depend on a case-by-case analysis, which can only be done by the tribunal. It seems that a good step would also include eliminating sensitive data before the data is processed for the arbitration’s context, as Kathleen Paisley defends.<sup>169</sup>

The fact is that arbitration is becoming more aware of the problems related to data protection (in general) and more references are being made in different documents. As an example, article 9(2) of IBA’s “Taking of Evidence in International Arbitration” foresees a number of reasons of why some kind of evidence might be excluded. One of them resides, precisely, on the “legal impediment or privilege under the legal or ethical rules determined by the Arbitral Tribunal to be applicable” (article 9(2)(b)) and “grounds of commercial or technical confidentiality that the Arbitral Tribunal determines to be compelling” (article 9(2)(e)). A commentary to IBA’s Rules foresees that personal data considerations may come under this limb. Nevertheless, it seems that a mere refuse *per se* is not admissible, unless it is possible to find a solid ground. Even when this happens, “the arbitral tribunal may order appropriate measures to preserve confidentiality of the evidence.”<sup>170</sup>

This can be articulated with the GDPR. In fact, attending to what the *privacy by design* demands, the controller has to implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and rights of data subjects (Article 25(1) of the GDPR). This provision aims to ensure that the controller takes into consideration the rights of the data subject from the beginning of the processing. On this

<sup>168</sup> Vide KATHLEEN PAISLEY, cit., p. 872.

<sup>169</sup> Ibid, p. 902.

<sup>170</sup> IBA, *Commentary on the Revised text of the 2020 IBA Rules on the Taking of Evidence in International Arbitration*, 2021, available <https://www.ibanet.org/MediaHandler?id=4F797338-693E-47C7-A92A-1509790ECC9D> (02.01.2024).

matter, A. Barreto Menezes Cordeiro outlines that this provision cannot be applicable to all situations that are directly or indirectly related with the processing, because in its opinion this would make article 24 GDPR useless.<sup>171</sup> Lee Bygrave states, on the other hand, that “the duty under article 25 expressly applies not just at the time of processing but also beforehand when the controller determines the means for processing.”<sup>172</sup> Additionally, *privacy by default* (Article 25(2) GDPR) prescribes that the “controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.” The latter is intrinsically related to the minimization and the extent of processing.<sup>173</sup>

Hence, whenever necessary, it is up to the controllers within the context of an arbitral processing to ensure all the adequate measures that are accepted by the GDPR and will allow to ensure the security of personal data (pseudonymization and mechanisms to ensure ongoing confidentiality, for example).<sup>174</sup> Nevertheless, in our opinion, it seems that is it not possible to use the GDPR as shield for the disclosure of documents. That permission would have a significant impact in the production of evidence within this proceeding and that is why, in our point of view, a case-by-case analysis will always be required, as well as – whenever necessary – additional measures should be adopted (but this will, of course, depend on the case itself). A cybersecurity and data protection approach will be essential. As David Rosenthal states, “if a party is not happy with the tribunal’s decision, it may raise data protection claims against the tribunal, or have a data subject do so.”<sup>175</sup>

### 3.3. Refusal of the Award on the Basis of GDPR’s violation

One last issue that we will further analyze is related to the question on whether it is possible to annul the award and refuse the recognition and enforcement on the basis of non-compliance with the GDPR. J. G. Merrills points out that “an arbitral award is binding, but not necessarily final”<sup>176</sup>. Nevertheless, it has to be mentioned that “the award is usually the outcome of arbitral proceedings that have been contested throughout.”<sup>177</sup> The question, if it is possible to challenge the award on the basis of the non-fulfillment of the GDPR, is not innocuous, as for the unsuccessful party that will be crucial.

Hence, this will depend on the different ways that this matter is regulated. Under a Non-ICSID Arbitration, the enforcement as a foreign award will occur under the New York Convention<sup>178</sup>,

<sup>171</sup> A. BARRETO MENEZES CORDEIRO, cit., p. 332.

<sup>172</sup> LEE A. BYGRAVE, “Article 25”, in CHRISTOPHER KUNER / LEE A. BYGRAVE / CHRISTOPHER DOCKSEY (ed.) *The EU General Data Protection Regulation (GDPR)*, Oxford, Oxford University Press, 2020, pp. 571-581(576).

<sup>173</sup> As GRAÇA CANTO MONIZ, cit., p. 221 prescribes, they are both complementary, which means that privacy by default depends of the privacy by design.

<sup>174</sup> See Article 32(1)(a)-(d) of the GDPR.

<sup>175</sup> DAVID ROSENTHAL, cit., p. 836.

<sup>176</sup> J. G. MERRILLS, *International Dispute Settlement*, Sixth Edition, Cambridge, Cambridge University Press, 2018, p. 106.

<sup>177</sup> NIGEL BLACKABY et. al, cit., p. 502.

<sup>178</sup> As January 2023, 172 State Parties have ratified the award.

setting-aside under the *lex arbitrii*. Article III of the Convention foresees that each contracting state shall recognize arbitral awards as binding and enforce them in accordance with the rules of procedure of the territory where the award is relied upon. Besides, article V consecrates a number of reasons why the enforcement of the award might be refused. The only one that can be equated is article V(2)(b), because the recognition or enforcement of the award contrary to the public policy of the country<sup>179</sup>.

There is, therefore, a difference between domestic and international public policy, because as Albert Jan Van Den Berg points out, “what is considered to pertain to public policy in domestic relations does not necessarily pertain to international policy in international relations.”<sup>180</sup> Even though there are not cases at the time, this does not mean that it will not be problematic in the near future.<sup>181</sup> Thus, we might ask ourselves if the GDPR’s articles can be considered public policy. We have to agree with the doctrine that defends that not all the provisions foreseen on the GDPR will allow this, as not all “obligations carry the same weight.”<sup>182</sup> Still, the ECJ might have an important impact in analyzing which kind of articles will play the decisive role. One example that can create several problems, and plays an important role in ensuring the free flow of data (and also respect data subject’s rights) is related to International Transfers. From what we have seen, it is very hard to allow for these transfers to happen, especially when we think about the USA – which, most likely, will create direct conflicts between the USA and EU. There is, as Alexander Blumrosen states, “a risk that EU Member State National courts could refuse enforcement of international arbitration awards that are based on unlawfully transferred personal data in violation of such rules in application of the public policy exception.”<sup>183</sup>

Regarding ICSID Convention, there is an automatic enforcement in any ICSID Parties. Therefore, each contracting state party shall recognize an award as binding and enforce the pecuniary obligations (see article 54(1) of ICSID Convention). Under article 52 of ICSID Convention, and contrarily to the New York Convention, no public policy exception is allowed. Looking at the reasons on which the parties may request the annulment of the award, it is quite hard to find something that might be suitable to this situation.<sup>184</sup> Having in mind all of these options, none seems adequate. As a last resource, it could be argued that there had been a serious departure from a fundamental rule of procedure, but again this will depend on the consideration of the data protection regulations as procedural or substantive law.<sup>185</sup>

<sup>179</sup> As NIGEL BLACKABY et. al, cit., p. 641, clarify states might wish to have the right to refuse, recognize or enforce the award on this basis, but it will be quite hard.

<sup>180</sup> ALBERT JAN VAN DEN BERG, *The New York Convention of 1958: An Overview*, [https://cdn.arbitration-icca.org/s3fs-public/document/media\\_document/media012125884227980new\\_york\\_convention\\_of\\_1958\\_overview.pdf](https://cdn.arbitration-icca.org/s3fs-public/document/media_document/media012125884227980new_york_convention_of_1958_overview.pdf) (02.02.2024).

<sup>181</sup> ALEXANDER BLUMROSEN, cit., p. 107.

<sup>182</sup> NEVA CIRKVENI / PER NEUBURGER, cit.

<sup>183</sup> ALEXANDER BLUMROSEN, cit., p. 109. *Vide* also DAVID M. HOWARD, cit., pp. 406-407.

<sup>184</sup> Article 52(1) of ICSID Convention foresees that the annulment of the award might occur on the basis of the following reasons, namely: that the Tribunal was not properly constituted; (b) that the Tribunal has manifestly exceeded its powers; (c) that there was corruption on the part of a member of the Tribunal; (d) that there has been a serious departure from a fundamental rule of procedure; or (e) that the award has failed to state the reasons on which it is based.

<sup>185</sup> NEVA CIRKVENI / PER NEUBURGER, cit..



The GDPR cannot be used as a way to react against decisions, just because the parties did not like the outcome. One final note should be made to the case *Eco Swiss China Time Ltd vs. Benetton International NV*<sup>186</sup>, where the ECJ held that the provisions of Article 81 EC (ex Article 85) may be regarded as a matter of public policy within the meaning of the New York Convention.<sup>187</sup> Thus, it after concluded that a national court where an application is made for annulment of an arbitration award must grant that application if it considers that the award in question is in fact contrary to Article 81 EC (ex Article 85) of the Treaty, where its domestic rules of procedure require it to grant an application for annulment founded on failure to observe national rules of public policy.<sup>188</sup> We shall see in the following years if any development on this regard is made.<sup>189</sup>

#### 4. A data protection agreement as a path to follow?

In order to prevent many of the issues analyzed throughout this essay, it may be necessary to put in place a data protection agreement, in order to address the requirements demanded by different legislations<sup>190</sup>, such as the GDPR. Kathleen Paisley states that this might take several forms. For example, party agreement, a stipulation or a tribunal order.<sup>191</sup> After all, in a case where the application of the GDPR is possible, it is essential to guarantee that not only the parties, as well as representatives, witnesses, experts, the tribunal, comply with the different provisions of the regulation.<sup>192</sup>

We cannot forget that a process of arbitration implies different flows of personal data processing<sup>193</sup> and, as we have already pointed out, this is a new issue. Thus, the provisions of the regulation are not helpful in order to know what to do in these situations. Additionally, the biggest advantage of this process is related to the increase of "arbitral efficiency while minimizing data protection risks."<sup>194</sup> Moreover, we say that this should be a practice inherent to all proceedings and not only the ones involved the GDPR, because there are multiple data protection laws on this matter. By doing their own Agreement, it will be easier for the parties, as well as the Tribunal to ensure that the GDPR is not used in a way to gain a certain advantage in the proceeding (for example, refuse an award on the basis of the non-fulfillment of the GDPR

<sup>186</sup> Court of Justice (CJ) *Eco Swiss China Time Ltd vs. Benetton International NV*, 1/06/1999, C-126/97

<sup>187</sup> Court of Justice (CJ) *Eco Swiss China Time Ltd vs. Benetton International NV*, 1/06/1999, C-126/97, paragraph 39.

<sup>188</sup> European Court of Justice (ECJ) *Eco Swiss China Time Ltd vs. Benetton International NV*, 1/06/1999, C-126/97, paragraph 41.

<sup>189</sup> ICCA-IBA, *Joint Task Force on Data Protection*, p. 63 does not address this issue. Instead, it focusses on the questions related to the processing of personal data that an award might have.

<sup>190</sup> DAVID ROSENTHAL, cit., pp. 836-838. KATHLEEN PAISLEY, cit., pp. 912-918.

<sup>191</sup> KATHLEEN PAISLEY, cit., pp. 912.

<sup>192</sup> CLARA-ANN GORDON, cit., p. 33.

<sup>193</sup> It is, as NIKOS LAVRANOS, "The Need for a Data Protection Protocol for Arbitration Proceedings", in *Practical Law Arbitration Blog*, 2019, available <http://arbitrationblog.practicallaw.com/the-need-for-a-data-protection-protocol-for-arbitration-proceedings/> (03.02.2024) points out, essential to "adopt pro-active measures in order to deal with the data protection issues in an efficient and effective way."

<sup>194</sup> KATHLEEN PAISLEY, cit., p. 913.

or refuse to present an evidence), as well as it might solve in advance some of the points that later will be problematic.

## 5. Conclusion

To sum up, throughout this article, we have seen how the GDPR impacts the proceeding of an International Arbitration. The reality is changing which day, not only in International Treaty Arbitration, as well as in International Commercial Arbitration. Moreover, different protocols are being adopted by the different tribunals, which is a clear sign of the growing significance that is being given to it. On the other hand, from a GDPR's point of view, it is clear that the proceeding of an international arbitration implies the processing of different personal data.

Additionally, we have seen how it might be tricky to consider the extraterritorial application of the GDPR, as some case law demonstrates a strict approach when it comes to know if the regulation can be applicable and many countries, even though some evolution has been made, do not have similar rules to the GDPR. Therefore, international data transfers are difficult, namely because the Commission hasn't adopted so many adequacy decisions so far, as well as article 46 and 49(2) seem difficult to be applicable. One last resource might reside on invoking article 49(1)(e) by demonstrating that the transfer is necessary for the establishment, exercise or defense of a legal claim.

Thus, and we enter the analysis of the GDPR itself, we may see how hard it is to articulate the rules with the needs of international arbitration, namely on regards to online hearings and evidence. In our point of view, when it is possible to apply the regulation, it is essential for the different processors and controllers to take into consideration the requirements demanded, but we do not think that the GDPR can be used as a "shield" for the different parties in order to maneuver the arbitration itself. There must be a solid and coherent ground on its application, by taking into consideration all the specifications inherent to international arbitration.

We do not know what the future holds, as it seems that only now we are starting to take more seriously data protection issues. In the future, the different tribunals will have to adapt themselves and, above all, be prepared for the digital transformation, which means that the GDPR will continue to play a crucial role in the following years. After all, in this new era, it seems that International Arbitration and Data Protection Law, will collide to offer a better approach of the law. The future starts now.

## Bibliography

- AFONSO, FILIPE GALVÃO TELES SANCHES, "The fifth arbitrator? The Role of Artificial Intelligence to Tribunals in International Arbitration", in *Revista Internacional de Arbitragem e Conciliação*, Volume XIII, 2020, pp. 147-188
- ALAMDARI, BAHAR HATAMI, "The Question of Remote Hearings in International Commercial Arbitration", in LALANI, SHAHEEZA / SHAPIRO, STEVEN G. (ed), *The Impact of Covid on International Disputes*, Leiden, Brill Nijhoff, 2022, pp. 141-156
- AYALA, MADALENA DINIS, "The Rising Inefficiency in Arbitration: is Technology the Solution?", in *Revista de International de Arbitragem e Conciliação*, Volume XVI, 2021, pp. 115-145
- BAJPAI, ANANYA / KALA, SHAMBHAVI, "Data Protection, cybersecurity and International Arbitration: Can they reconcile?", in *Indian Journal of Arbitration Law*, Volume 8, Issue 2, 2020, pp. 1-18
- BARBOSA, MAFALDA MIRANDA, "Do Juiz Árbitro ao software juiz árbitro: uma evolução possível?", in *Revista Internacional de Arbitragem e Conciliação*, Volume XIII, 2020, pp. 37-64
- BERG, ALBERT JAN VAN DEN, *The New York Convention of 1958: An Overview*, [https://cdn.arbitration-icca.org/s3fs-public/document/media\\_document/media012125884227980new\\_york\\_convention\\_of\\_1958\\_overview.pdf](https://cdn.arbitration-icca.org/s3fs-public/document/media_document/media012125884227980new_york_convention_of_1958_overview.pdf) (02.02.2024)
- BERMANN, GEORGE A., "The Future of International Commercial Arbitration", in LIM, C. L. (ed) *The Cambridge Companion to International Arbitration*, Cambridge, Cambridge University Press, 2021, pp. 138-175
- BIENVENU, PIERRE / GRANT, BENJAMIN, "Data Protection and Cyber risk issues in Arbitration", in *International Arbitration Report*, Issue 13, Norton Rose Fulbright, 2019, pp. 19-21
- BLACKBABY, NIGEL, et. al., *Redfern and Hunter on International Arbitration*, Oxford, Oxford University Press, 2015
- BLUMROSEN, ALEXANDER, "The Allocation of GDPR Compliance in Arbitration", in DONA, JOSÉ R. MATA DONA / LAVRANOS, NIKOS (ed) *International Arbitration and EU Law*, Cheltenham, Edward Elgar Publishing, 2021, pp. 92-109
- BYGRAVE, LEE. A., "Article 25", in KUNER, CHRISTOPHER / BYGRAVE, LEE A. / DOCKSEY, CHRISTOPHER (ed), *The EU General Data Protection Regulation (GDPR)*, Oxford, Oxford University Press, 2020, pp. 571-581
- CARVALHO, JORGE MORAIS, *Direito do Consumo*, 7.º Edition, Coimbra, Almedina, 2021
- CIRKEVENI, NEVA / NEUBURGER, PER, "Clash of the Titans: GDPR and International Arbitration – A Look at the Future", *Rechtsanwälte Attorneys Law*, 2021, available <https://oblin.at/publication/clash-of-the-titans-gdpr-and-international-arbitration-a-look-at-the-future/> (13.09.2023)

COHEN, STEPANIE / MORRIL, MARK, "A Call to Cyberarms: The International Arbitrator's duty to avoid digital intrusion", in *Fordham International Law Journal*, Volume 40, Issue 3, pp. 981-1022

CORDEIRO, A. BARRETO MENEZES, "Dados Pessoais: conceito, extensão e limites", in *Revista de Direito Civil*, Ano 3, Volume 2, 2018, pp. 297-321

CORDEIRO, A. BARRETO MENEZES, *Direito da Proteção de Dados à luz do RGPD e da Lei n.º 58/2019*, Coimbra, Almedina, Reimpressão, 2020

CORDEIRO, A. BARRETO MENEZES, "Artigo 2.º", in CORDEIRO, A. BARRETO MENEZES (Coord.) *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Coimbra, Almedina, 2021, pp. 66-70

CORDEIRO, A. BARRETO MENEZES, "Artigo 3.º", in CORDEIRO, A. BARRETO MENEZES (Coord.) *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Coimbra, Almedina, 2021, pp. 70-77

DOUGLAS, ZACHARY, "The Hybrid Foundations of Investment Treaty Arbitration", in *British YearBook of International Law*, Volume 74, Issue 3, 2003, pp. 151-289

EGAN, MO / YU, HONG-LIN, "Intersecting and Dissecting Confidentiality and Data Protection in Online Arbitration", *Journal of Business Law* (forthcoming), 2022, pp. 1-27, available at <https://dspace.stir.ac.uk/handle/1893/31758> (29.04.2024)

FRANCK, SUSAN D., "The Legitimacy Crisis in Investment Treaty Arbitration: Privatizing Public International Law Through Inconsistent Decisions", in *Fordham Law Review*, Volume 73, Issue 4, 2005, pp. 1521-1625

GEORGAKI, KONSTANTINA, "Conflict Resolution between EU Law and Bilateral Investment Treaties of the EU Member States in the Aftermath of Achmea", in *Yearbook of European Law*, 2023, pp. 1-27, available <https://doi.org/10.1093/yel/yeac012> (19.09.2023)

GIUPPONI, BELEN OLMOS, "Virtual Dispute Resolution in International Arbitration – Mapping its advantages and main caveats in the Face of Covid-19", in LALANI, SHAHEEZA / SHAPRIO, STEVEN G. (ed) *The Impact of Covid on International Disputes*, Leiden, Brill Nijhoff, 2022, pp. 62-83

GORDON, CLARA-ANN, "The Impact of GDPR on International Arbitration – a Practical Guideline", in *Dispute Resolution Journal*, Volume 74, Issue 4, 2019, pp. 27-34

HAY, EMILY, "The Invisible Arm of the GDPR in International Treaty Arbitration: Can't we make it go away?", in *Kluwer Arbitration Blog*, 2019, available <https://arbitrationblog.kluwerarbitration.com/2019/08/29/the-invisible-arm-of-gdpr-in-international-treaty-arbitration-cant-we-make-it-go-away/> (11.11.2023)

HENRY, MARC, "An Arbitrator's Perspective: Confidentiality – Privacy – Security in the Eye of the Arbitrators or the Story of the Arbitrator who Became a Bee", in VICENTE, DÁRIO MOURA VICENTE / OLIVEIRA, ELSA DIAS / ALMEIDA, JOÃO GOMES DE (ed) *Online Dispute Resolution – New Challenges*, Baden-Baden, Nomos, 2022, pp. 181-204

- HIRSCH, DENNIS D., “The Glass House Effect: Big Data, The New Oil and the Power of Analogy”, in *Maine Law Review*, Volume 66, 2014, pp. 373-495
- HOUSER, KIMBERLY A. / BAGBY, JOHN W., “The Data Trust Solution to Data Sharing Problems”, *Vanderbilt Journal of Entertainment & Technology Law*, Volume 25, Issue 1, 2023, pp. 113-180
- HOWARD, DAVID, “Foreign Data Protection in International Arbitration and United States Litigation”, in *Texas International Law Journal*, Volume 55, Issue 3, pp. 395-407
- HUANG, JIE Jeanne, “Conflicts and Tentative Solutions to Protecting Personal Data in Investment Arbitration”, in *The European Journal of International Law*, Volume 32, no. 4, 2021, pp. 1191-1220
- HUANG, JIE JEANNE / XIE, DAN, “Data Protection Law in Investment Arbitration: Applicable or Not?”, in *Arbitration International* (forthcoming), pp. 1-47, 2021, available [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3763222](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3763222) (02.10.2023)
- KELLEHER, DENIR / MURRAY, KAREN, *EU Data Protection Law*, London, Bloomsbury Professional, 2018
- KLAR, MANUEL, “Art. 3 Raumlicher Anwendungsbereich”, in KÜHLING, JÜRGEN / BUCHNER, BENEDIKT (ed), *Datenschutz-Grundverordnung/BDSG Kommentar*, 2.<sup>a</sup> Auflage, Munich, C.H. BECK, 2018, pp. 109-137
- KRANENBORG, HERKE, “Article 2 Material Scope”, in KUNER, CHRISTOPHER / BYGRAVE, LEE A. / DOCKSEY, CHRISTOPHER (ed), *The EU General Data Protection Regulation (GDPR)*, Oxford, Oxford University Press, 2020, pp. 60-73
- KUNER, CHRISTOPHER, “Article 45. Transfers on the basis of an adequacy decision”, in KUNER, CHRISTOPHER / BYGRAVE, LEE A. / DOCKSEY, CHRISTOPHER (ed), *The EU General Data Protection Regulation (GDPR)*, Oxford, Oxford University Press, 2020, pp. 771-796
- LANDI, NICCOLÒ, “Remote Hearings: Observations on the Problem of Personal Data Protection and Cybersecurity”, in *Does a Right to a Physical Hearing Exist in International Arbitration?*, *International Council for Commercial Arbitration*, 2022, pp. 127-165, available <http://www.arbitration-icca.org/> (12.12.2023)
- LAVRANOS, NIKOS, “The Need for a Data Protection Protocol for Arbitration Proceedings”, in *Practical Law Arbitration Blog*, 2019, available <http://arbitrationblog.practicallaw.com/the-need-for-a-data-protection-protocol-for-arbitration-proceedings/> (03.02.2024)
- MAZETOVA, ELENA, “Data Protection Regulation and International Arbitration: Can There be Harmonious Coexistence (with the GDPR Requirements Concerning Cross Border Data Transfer?)”, in *Legal Issues in the Digital Age*, 2/2021, 2021, pp. 21-48
- MERRILIS, J. G., *International Dispute Settlement*, Sixth Edition, Cambridge, Cambridge University Press, 2018
- MONIZ, GRAÇA CANTO, *Manual de Introdução à Proteção de Dados*, Coimbra, Almedina, 2023

PAISELY, KATHLEEN, “It’s All about the Data: The Impact of the EU General Data Protection Regulation on International Arbitration”, in *Fordham International Law Journal*, Volume 41, Issue 4, 2018, pp. 841-936

PINHEIRO, ALEXANDRE SOUSA / GONÇALVES, CARLOS JORGE, “Artigo 45.º Transferências com base numa decisão de adequação”, in PINHEIRO, ALEXANDRE SOUSA et. al. (ed) *Comentário ao Regulamento Geral de Proteção de Dados*, Coimbra, Almedina, 2018, pp. 504-512

PINHEIRO, ALEXANDRE SOUSA / GONÇALVES, CARLOS JORGE, “Artigo 49.º Derrogações para situações específicas”, in PINHEIRO, ALEXANDRE SOUSA et. al. (ed) *Comentário ao Regulamento Geral de Proteção de Dados*, Coimbra, Almedina, 2018, pp. 524-530

POLLICINO, ORESTE / BASSINI, MARCO / GREGORIO, GIOVANNI DE, *Internet Law and the Protection of Fundamental Rights*, Bocconi, Bocconi University Press, 2022

POULSEN, LAUGE N. SKOVGAARD, “The Investment Treaty Arbitration”, in PEVEHOUSE, JON C. W. / SEABROOKE, LEONARD (ed) *The Oxford Handbook of International Political Economy*, Oxford, Oxford University Press, 2021, available <https://doi.org/10.1093/oxfordhb/9780198793519.013.26> (accessed 01.05.2023)

ROSENTHAL, DAVID, “Complying with the General Data Protection Regulation (GDPR) in International Arbitration – Practical Guidance”, in *Asa Bulletin*, Volume 37, Issue 4, 2019, pp. 822-837

SHARMA, TANMAYI, “Evidence in International Arbitration: Admissibility, Relevance and Differences between Common and Civil Law”, in *Católica Law Review*, Volume II, n.º 2, 2018, pp. 99-113

STACH, CHRISTOPH, “Data is the New Oil-Sort of: A View on Why this comparison is misleading and its implications for Modern Data Administration”, in *Future Internet*, 15, 71, 2023, pp. 1-49, available <https://doi.org/10.3390/fi15020071> (13.11.2023)

SVANTESSON, DAN, “Article 3. Territorial Scope”, in KUNER, CHRISTOPHER / BYGRAVE, LEE A. / DOCKSEY, CHRISTOPHER (ed), *The EU General Data Protection Regulation (GDPR)*, Oxford, Oxford University Press, 2020, pp. 74-99

TEIXEIRA, DINA FREITAS, “Artigo 45.º Transferência com base numa decisão de adequação”, in CORDEIRO, A. BARRETO MENEZES (Coord.) *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Coimbra, Almedina, pp. 320-328

TEIXEIRA, DINA FREITAS, “Artigo 46.º. Transferências Sujeitas a Garantias Adequadas”, in CORDEIRO, A. BARRETO MENEZES (Coord.) *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Coimbra, Almedina, pp. 329-336

TERWANGNE, CÉLIE DE, “Article 5: Principles Relating to processing of personal data”, in KUNER, CHRISTOPHER / BYGRAVE, LEE A. / DOCKSEY, CHRISTOPHER (ed), *The EU General Data Protection Regulation (GDPR)*, Oxford, Oxford University Press, 2020, pp. 309-320

VISCASILLAS, PILAR PERALES, “An Arbitrator’s Perspective: Online hearings in Arbitration: the taking of Evidence”, in Vicente, Dário Moura / Oliveira, Elsa Dias / Almeida, João Gomes de (ed) *Online Dispute Resolution New Challenges*, Baden-Baden, Nomos, 2022, pp. 107-131

VICENTE, MARTA, “The European Union’s Proposal for the Modernization of the Energy Charter Treaty”, in *European Energy and Environmental Law Review*, Volume 31, Issue 3, 2022, pp. 124-134

VOSS, W. GREGORY / HOUSER, KIMBERLY A., “Personal Data and the GDPR: Providing a Competitive Advantage for U.S Companies”, in *American Business Law Journal*, Volume 56, Issue 2, pp. 287-344

ZAHARIEV, MARTIN, “Mission (im)possible: Where GDPR Meets Commercial Arbitration”, in KLAUSEGGER, CHRISTIAN et. Al. (ed) *Austrian Yearbook on International Arbitration*, Bern, C.H. Beck, 2020, pp. 3-21

## Relevant Documents

AMERICAN ARBITRATION ASSOCIATION-INTERNATIONAL CENTER FOR DISPUTE RESOLUTION, *Virtual Hearing Guide for Arbitrators and Parties*, adopted on 9<sup>th</sup> may 2020

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 4/2007 on the concept of personal data*, adopted on 20<sup>th</sup> June 2007

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working Document 1/2009 on pre-trial discovery for cross border civil litigation*, adopted on 11<sup>th</sup> February 2009

EUROPEAN DATA PROTECTION BOARD, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, adopted on 25<sup>th</sup> May 2018

EUROPEAN DATA PROTECTION BOARD, *Guidelines 3/2018 on the territorial scope of the GDPR*, adopted on 16<sup>th</sup> November 2018

EUROPEAN DATA PROTECTION BOARD, *Guidelines 3/2021 on the territorial scope of the GDPR (Article 3)*, adopted on 7<sup>th</sup> January 2020.

EUROPEAN DATA PROTECTION BOARD, *Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1*, adopted on 4<sup>th</sup> May 2020

EUROPEAN DATA PROTECTION BOARD, *Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default*, adopted on 20<sup>th</sup> October 2020

HONG KONG INTERNATIONAL ARBITRATION CENTER, *Guidelines for Virtual Hearings*, adopted on 15<sup>th</sup> May 2020, available <https://www.hkiac.org/news/hkiac-guidelines-virtual-hearings> (02.12.2023)

INTERNATIONAL BAR ASSOCIATION, *Rules on the Taking of Evidence in International Arbitration*, adopted on 17<sup>th</sup> December 2020, available <https://www.ibanet.org/> (13.11.2023)

INTERNATIONAL BAR ASSOCIATION, *Commentary on the Revised text of the 2020 IBA Rules on the Taking of Evidence in International Arbitration*, 2021, available <https://www.ibanet.org/MediaHandler?id=4F797338-693E-47C7-A92A-1509790ECC9D> (02.01.2024)

INTERNATIONAL COUNCIL FOR COMMERCIAL ARBITRATION / INTERNATIONAL BAR ASSOCIATION, *Joint Task Force on Data Protection in International Arbitration – Roadmap to Data Protection in International Arbitration*, 2022, available <https://www.arbitration-icca.org/icca-reports-no-7-icca-iba-roadmap-data-protection-international-arbitration> (15.10.2023).

INTERNATIONAL COUNCIL FOR COMMERCIAL ARBITRATION / INTERNATIONAL BAR ASSOCIATION / NEW YORK CITY BAR / INTERNATIONAL INSTITUTE FOR CONFLICT PREVENTION & RESOLUTION, *Protocol on Cybersecurity in International Arbitration*, 2022, available [https://cdn.arbitration-icca.org/s3fs-public/document/media\\_document/ICCA-reports-no-6-icca-nyc-bar-cpr-protocol-cybersecurity-international-arbitration-2022-edition.pdf](https://cdn.arbitration-icca.org/s3fs-public/document/media_document/ICCA-reports-no-6-icca-nyc-bar-cpr-protocol-cybersecurity-international-arbitration-2022-edition.pdf) (15.10.2023)

KOREAN COMMERCIAL ARBITRATION BOARD, *Seoul Protocol on Video Conferencing in International Arbitration*, adopted on 18<sup>th</sup> March 2020

## Cases

European Court of Justice (ECJ) *Eco Swiss China Time Ltd vs. Benetton International NV*, 1/06/1999, C-126/97

European Court of Justice (ECJ), *Lindqvist*, 06/11/2003, C-101/01

European Court of Justice (ECJ), *Maximilian Schrems v. Data Protection Commissioner (Schrems I)*, 6/10/2015 C-362/14

European Court of Justice (ECJ), *B v. Latvijas Republikas Saeima*, 22/06/2021, C-439/19

European Court of Justice (ECJ), *Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems (Schrems II)*, 16/07/2020, C-311/18

European Court of Justice (ECJ), *Norra Stockholm Bygg AB v. Per Nycander AB, Entral AB*, 02/03/2023, C-268/21

International Center for Settlement of Investment Disputes (ICSID), *ConocoPhillips v. Venezuela*, no. ARB/07/30.

*Decision on Respondent's Request for Reconsideration*, 10 March 2014, available at <https://www.italaw.com/sites/default/files/case-documents/italaw3119.pdf> (19.11.2023)



Permanent Court of Arbitration (PCA), *Tenant Energy, LLC v. Government of Canada*, no. 2018-54

*Claimant's E-mail to the Tribunal regarding the Application of the EU GDPR*, 2019, available at <https://www.italaw.com/cases/7250> (20.10.2023)

*Respondent's Letter to the Tribunal regarding EU GDPR*, 2019, available at <https://www.italaw.com/cases/7250> (accessed 25.10.2023).

*Questions and Claimant's Response to the Tribunal GDPR Questions and Data Privacy*

*Questions*, 2019, available at <https://www.italaw.com/cases/7250> (26.10.2023)

*Tribunal's Communication to the Parties*, 2019, available <https://www.italaw.com/cases/7250> (29.10.2023)

Permanent Court of Arbitration (PCA), *Elliott Associates, L.P. (USA) v. Republic of Korea*, No. 2018-51

## Legislation

International Chamber of Commerce Rules of Arbitration, 1 January 2021

London Court International Arbitration Rules, 1 October 2020

Regulation (EU) 2016/679 of the European Parliament of the Council, 27 April 2016

UNCITRAL Arbitration Rules, General Assembly Resolution 31/98

Vienna International Arbitral Center Rules and Mediation, 1 July 2021

(texto submetido a 16.02.2024 e aceite para publicação a 12.04.2024)