Data Protection Regulation and International Arbitration: Can There Be Harmonious Coexistence (with the GDPR Requirements Concerning Cross-Border Data Transfer)?

Elena Mazetova

Lecturer, Department of International Law, National Research University Higher School of Economics, LL.M. Address: 20 Myasnitsky Str., Moscow 10100, Russia. E-mail: emazetova@hse.ru

Abstract

Recent global trends are producing powerful growth in the digital environment, and its spread is prompting adoption of strict and comprehensive regulation to ensure data protection. This results in a number of difficulties, one of which is lack of consistency between data protection regulation and the regulatory regimes applicable to specific industries and institutions. That inconsistency is particularly evident in the field of international arbitration — one of the most widely used and convenient methods for resolving international disputes. The principles and fundamental concepts that largely define international arbitration, such as autonomy of the parties and confidentiality, have made its use very well accepted and widespread. However, data protection requirements often force the parties that are subject to them to make a difficult choice between the basic principles of international arbitration and the requirements of data protection regulation. This bind has come about because data protection regulation, which generally imposes comprehensive compliance obligations, rarely takes into account the specifics of the industries in which it will be applied. In this article it is analyzing application of the GDPR requirements that pertain to cross-border data transfer from the perspective of international arbitration in order to illustrate difficulties and regulatory gaps that may be encountered by the entities interested in thorough compliance with the applicable regulations.

Keywords

private data, data protection, cross-border data transfer, GDPR, international arbitration, legal claims, legal proceedings.

For citation: Mazetova E. A. (2021) Data Protection Regulation and International Arbitration (Can There Be Harmonious Coexistence?) *Legal Issues in the Digital Age,* no 2, pp. 21–48.

DOI: 10.17323/2713-2749.2021.2.21.48

Introduction

The idea that private data needs to be protected is not new: it stems largely from Semayne's case (in which it was declared that "the house of every one is to him as his castle and fortress")[1] [Cooper D., Kuner C., 2017: 44] and has undergone a lengthy path of development since then.[2] People have ultimately become much more aware of the importance of protecting their private life and, as a logical extension, of guarding their personal data, but the explosive development of technology has made protecting data a challenging task that requires consideration of various nuances.

The problems attendant upon pervasive digitalization are now being widely discussed at a time when the standard way of saving and sharing information is transitioning from paper to digital formats and most processes and communications are going online, and it is well accepted that the numerous benefits from increasing use of technology usage also entail significant risks. Undoubtedly, the trend toward digitalization has been significantly reinforced and accelerated by the COVID-19 pandemic, and it is unlikely that this progression toward a digital reality can be reversed in the future. As a result, we face a dramatic increase in the types and amount of data, including data of private individuals, which is constantly being collected, stored and transmitted on various (and also continually proliferating) types of devices [Burianski M., Reindl M., 2010: 183].

In this context it is not surprising that data protection issues are attracting increased attention from state actors,[3] which then results in the development of more advanced and complex data protection regulations.[4] It is notable

[1] See Semayne's case, 77 Eng. Rep. 194 (Kb 1604).

[2] The idea of data privacy was elaborated thoroughly by Samuel Warren and Louis Brandeis in their article of 1890 published in the *Harvard Law Review*.

[3] For example, the Brazilian General Data Protection Law. Available at: https://gdpr.eu/gdpr-vs-lgpd/ (accessed: 20.04.2021). Another example is the California Consumer Privacy Act. Available at: https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do (accessed: 20.04.2021)

[4] According to data from the United Nations Conference on Trade and Development, only 19% of countries across the globe have no special data protection and privacy regulations. Available at: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (accessed: 20.04.2021)

that the recently growing interest of states in regulating data protection issues also points up another trend in digitalization, which is the increased speed and technical simplicity of transferring data between different countries. This trend is understandably welcomed by commercial companies (in particular, those that conduct their business at the international level); however, it is causing heightened concern on the part of regulators. The upshot is that states want their data protection standards to apply across jurisdictional borders or else to significantly restrict transfers of data across those borders [Cooper D., Kuner C., 2017: 32–33, 72], and this influences the approaches to data protection legislation adopted by the respective states.

It is also noteworthy that, although large IT corporations such as Google or Facebook are seen as the main "addressees" of recent data protection regulation, we find that even companies whose main business is not directly related to the internet or development of technology are facing significant fines for violation of data protection laws.[5] Thus, it is fair to say that data protection regulation is becoming truly comprehensive and influencing almost all areas of life by requiring the key actors responsible for collecting and processing private data to apply additional safeguards and protections.

As will be shown below, all these circumstances have led to conflicting requirements, not only within the field of data protection itself (and in particular as it affects cross-border aspects) but also between data protection regimes and other areas of law, e.g. international arbitration. Those areas of law normally have their own rules and principles of operation, but at the same time they are not exempt from the application of data protection requirements. As Christopher Kuner correctly indicated, this incompatibility between different legal regimes may "go beyond simple conflict of laws, and can be viewed as conflicts between different social sectors" (Kuner C., 2013: 135).

International arbitration provides a good example of this kind of conflict: first, it is a rapidly developing and widely used tool for resolving international disputes. Almost any company that conducts business across borders has either already resorted to international arbitration in order to resolve disputes or may potentially need to do so.[6] Second, although inter-

[5] For example, a £18.4 million fine was imposed on Marriott International Inc. for a data protection breach (ICO Penalty Notice. 30 October 2020, case ref.: COM0804337. Available at: https://ico.org.uk/action-weve-taken/enforcement/marriott-international-inc/ (accessed: 06.04.2021)). A similar fine of £20 million was levied against British Airways (ICO Penalty Notice.16 October 2020, case ref.: COM0783542. Available at: https://ico.org.uk/action-weve-taken/enforcement/british-airways/ (accessed: 06.04.2021)

[6] International arbitration was considered the preferred method of dispute resolution by 97% of respondents to the 2018 International Arbitration Survey: The Evolution of In-

national arbitration understood as a branch of law is far removed from the field of data protection, it is still significantly affected by it and in practice is often forced to adapt to data protection rules.

In the analysis that follows, we will focus on the application of data protection regulations to international arbitration and will consider certain difficulties and inconsistencies that parties to international arbitration may encounter in their attempt to comply with data protection requirements.

1. How data protection regulation affects international arbitration

As mentioned above, the growing concern about data protection could not fail to impact nearly every aspect of life and business operations.[7] Because international arbitration is one of the most commonly used and convenient methods for resolution of international disputes, it should come as no surprise that it was affected both by the application of regulations concerning cross-border data transfer and also by the current trend toward data protection in general.

The impact becomes even more significant due to the recent development of online arbitration, as well as to the increasing penetration of digital tools and techniques into the conduct of arbitration proceedings.[8] Furthermore, the risks associated with cross-border data transfer become very meaningful in practice when international arbitration brings together participants from different jurisdictions who travel across the world and represent companies from different countries [Pastore J., 2017: 1029]. Each and every of those participants may be exposed to risks that could undermine the entire arbitration process [Cohen S., Morril M., 2017: 1005].

Although it may be argued that those risks are limited by the inherent confidentiality of arbitration and also by a consent-based and generally balanced approach to the production of documents and information in arbitration [Born G., 2021: 2495–2496], experience shows that international

ternational Arbitration, which was conducted by the School of International Arbitration at Queen Mary University of London in partnership with White&Case LLP.

[7] For instance, question related to the GDPR influence over the arbitration was one of those that the tribunal had to evaluate in *Tennant Energy LLC* v *Government of Canada* (see: *Tennant Energy, LLC* v *Government of Canada*, PCA case No. 2018-54).

[8] The Queen Mary University survey also shows that at least 61% of respondents highlight the "increased efficiency, including through technology" and that such measures as videoconferencing and hearing room technologies are always or frequently used by over 60% of respondents.

arbitration, as well as the parties involved in it, are encountering instances of data breaches with increasing frequency. The risks are incurred in a wide range of circumstances that include mistakenly sending personal information of one of the parties to a person not connected with the proceedings [Smeureanu I., 2011: 183–184],[9] leakage of clients' private data from law firms [Cohen S., Morril M., 2017: 987]; along with targeted hacker attacks on arbitration institution (e.g., as happened to the Permanent Court of Arbitration in the Hague in July 2015 in the course of hearing *The Republic of the Philippines* v *The People's Republic of China*) (Pastore J., 2017: 1023, 1026).

The risks to which private data may be exposed[10] in the process of international arbitration — which is clearly not risk-free — are a sufficient practical justification of applying data protection measures.

The need for the entities involved in international arbitration to comply with data protection requirements arises also from the data protection laws themselves. First, laws in that field typically offer a definition of "data processing" (as an activity which entails application of data protection regulation) so broad that almost any activity or process occurring in the course of resolving a dispute by an arbitration tribunal, from taking initial evidence to issuing an arbitral award, may fall within the scope of data protection requirements[11] and so trigger specific compliance obligations.

Second, although most of the recent data protection requirements exempt judicial proceedings from some group of obligations or from specific obligations, arbitration is not mentioned explicitly.[12] It is difficult to understand the reasoning behind this approach (there are as yet no official

[9] See, for example, the claim of an individual, Mr. Carlos Antonio, brought against an arbitration institution in Spain. As a result of a data breach, the arbitral institution was fined €6,000 for infringement of its obligation to protect data and confidentiality.

[10] It should be noted that a risk-based approach is also suggested by data protection regulations themselves, such as the GDPR, which highlights the importance of evaluating risks. Available at https://iapp.org/resources/article/the-risk-based-approach-in-the-gdpr-interpretation-and-implications/ (accessed: 10.04.2021)

[11] For example, in according with Art. 4(2) of the GDPR "processing" is defined as "any operation … which is performed on personal data…, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

[12] See, for example, Art. 23(f) of the GDPR; also see discussion of the Indian Draft Personal Data Protection Bill. Available at: http://arbitrationblog.kluwerarbitration.com/2019/04/16/data-protection-in-india-and-arbitration-key-questions-ahead/ (accessed: 23.04.2021)

comments or guidance that would explain it), but it leads naturally to discussion of the applicability of the existing exceptions to arbitration due to its mixed nature, which combines jurisdictional and contractual features [Lew J., Mistelis L., Kroll M., 2003: 72]. Nevertheless, commentators generally agree that a conservative approach which interprets the term "judicial proceedings" in a narrow sense as covering only state courts should prevail [Paisley K., 2018: 857].

As matters now stand, parties to arbitration cannot rely on the general exceptions and are forced to apply more nuanced, case-by-case analysis in order to properly comply with data protection regulations.

As a result, many reputable and respected arbitration institutions regularly update their rules and recommendations to the parties and tribunals involved in order to properly address data protection considerations.[13] Parallel to that, the professional community of lawyers are working on determining the best practices to ensure accurate and comprehensive compliance.[14] The importance of those efforts cannot be overestimated: the ICCA-IBA Roadmap to Data Protection in International Arbitration indicated that it is intended "to help arbitration professionals better understand the data protection and privacy obligations to which they may be subject in relation to international arbitration proceedings".[15] Nevertheless, the broad question of whether international arbitration and data protection regulations can coexist in harmony remains open. As will be further illustrated by the example of the EU's General Data Protection Regulation (hereinafter GDPR),[16] the lack of clarity on this matter means that the that parties to international arbitration and the other participants in it must continually choose between non-compliance (or at least improper compliance) with

[13] See, for example, Art. 30A of the LCIA Arbitration Rules 1 October 2020; or Section D "Protection of Personal Data" in the ICC Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration under the ICC Rules of Arbitration.1 January 2019.

[14] See, for example, the Cyber Security Guidelines from the IBA's Presidential Task Force on Cyber Security, October 2018. Available at: https://www.ibanet.org/LPRU/cybersecurity-guidelines.aspx (accessed: 23.04. 2021); the ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration, 2020. Available at: https://www.arbitration-icca.org/projects/Cybersecurity-in-International-Arbitration.html (accessed: 20.04. 2021); the Consultation Draft of the ICCA-IBA Roadmap to Data Protection in International Arbitration, February 2020. Available at: https://www.arbitration-icca.org/icca-reports-no-7-icca-iba-roadmap-data-protection-international-arbitration (accessed: 20.04.2021)

[15] See the ICCA-IBA Roadmap to Data Protection in International Arbitration, p. 1.

[16] Regulation (EU) 2016/679 of the European Parliament and of the Council 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

data protection requirements and securing all the potential benefits of international arbitration.

2. How the GDPR rules on cross-border data transfer affect international arbitration

It is pertinent to note that the recent global trends in data protection regulation have been set in motion largely by the GDPR, which entered into force in 2018.[17]

The worldwide acquiescence to the GDPR is due not only to the heavy fines (up to 4% of global gross revenue or €20 million) and possible criminal liability for violation of the GDPR, but also to its broad application and potentially extraterritorial effect.[18] The EU Commission made clear the extraterritorial ambition of the GDPR when it stated that "the primary purpose of these rules is to ensure that when the personal data of Europeans are transferred abroad, the protection travels with the data".[19] The approaches employed by the GDPR have also been adopted and reproduced in the legislative acts of other countries [Cooper D., Kuner C., 2017: 48). In a sense, the GDPR has prompted extensive reconsideration and improvement of data protection regimes in general, and it still remains one of the most comprehensive and detailed regulatory tools for personal data protection.

For this reason, we will examine in detail some of the data protection issues in international arbitration that have resulted from the rules promulgated by the GDPR. It should be noted that the overall impact of data protection regulation on international arbitration is significant and that it affects a wide variety of procedural matters, such as additional obligations for arbitrators and arbitral institutions [Cohen S., Morril M., 2017: 997–1002], issues with production of evidence [Cooper D., Kuner C., 2017: 100], difficulties with publication of awards [Tshanz P.-Y., 2006], etc. However, in this article we will primarily focus on analysis of the rules and grounds for cross-border data transfer: this regulatory nexus is particularly interesting

[17] The GDPR replaced the previous Data Protection Directive (Directive 95/46/EC), which had been in effect since 1995. See: The History of the General Data Protection Regulation. Available at: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (accessed: 04.05.2021)

[18] Communication from the EU Commission to the European Parliament and the / Council, Exchanging and Protecting Personal Data in a Globalised World, COM/ 2017/07 final. 10.01.2017. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/? uri= COM%3A2017% 3A7%3AFIN (accessed: 29.04.2021) (hereinafter EU Communication).

[19] Ibid.

because it highlights the underlining ideas peculiar to each of the regulatory fields under consideration while it also exposes discrepancies even at this basic conceptual level. We find several reasons for this particular problem.

First, the GDPR maintains that, once private data of EU data subjects is involved, data protection compliance may be required from almost everyone engaged in a case, including the principal parties themselves, counsels acting on their behalf, arbitral institutions (when applicable), members of the arbitral tribunal, and so on regardless of the home jurisdiction of any of these participants [Paisley K., 2018: 854].

Second, applying specific data protection rules, including the GDPR, in international arbitration is complicated by jurisdictional diversity, such that one party may be from one of the EU countries and another from Africa, the arbitral institution may be seated in an Asian country, the tribunal is composed of three arbitrators from three different jurisdictions, and hearings take place in various locations, etc. These geographically and jurisdictionally fragmented features of international arbitration mean that rules for cross-border data transfer will inevitably apply to international arbitration, but those rules will also be applied differently in each individual episode of data transfer.

Presumably, analysis of the cross-border data transfer regulations and identification of those that are applicable to a given situation should be the first step in preparing for arbitration, as it would determine the scope of possible disclosure and the sequence of actions required to comply with data protection regulations. It would be reasonable to expect that this first step should be rather straightforward and provide the parties with clear guidance concerning the applicable rules and potential risks. However, as will be demonstrated below, the reality may differ from expectations.

General GDPR requirements for cross-border data transfer

The GDPR regulates cross-border data transfer (i.e. transfer of data outside the European Economic Area [EEA])[20] and application of its rules in international arbitration is difficult to avoid. Requirements of the GDPR may come into play in various scenarios: for instance, when a party, either as a result of being registered within the EU[21] or due to processing or con-

[20] Actual list of the EEA countries available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:European_Economic_Area_(EEA) (accessed: 10.06.2021)

[21] See Art. 3 of the GDPR.

trolling data of EU individuals,[22] must decide whether to use or disclose documents containing that data to a tribunal (be it as a part of the party's written submission, evidence requested by the tribunal, or in any other form); or perhaps that data is to be disclosed to the opposing party from a different jurisdiction so that a suitable justification for transferring that data would be required.

In dealing with these issues in international arbitration, the parties should keep in mind the complex data protection environment created by the GDPR, which consists of a combination of prohibitions, limitations and data protection standards in which each layer is important for legitimate cross-border data transfer [Paisley K., 2018: 854–855].

The general rule provided by the GDPR is based on prohibition of data transfer outside the EEA, except for a limited number of circumstances in which it is expressly permitted.[23] In fact, a list of those limited occasions (or grounds) established by the GDPR may be divided into general restrictions[24] and specific derogations [Paisley K., 2018: 878–881].[25] In addition, the GDPR establishes the specific requirement to adhere to the data protection standards irrespective of the justification employed for data transfer.[26]

The list of grounds that make cross-border data transfer permissible is provided in Articles 45–49 of the GDPR. The method for applying these grounds follows the so-called "cascade principle" [Paisley K., 2018: 878], meaning that each ground for data transfer is to be analyzed one by one and each one applied only if the preceding one was found not suitable.

The first group of grounds for cross-border data transfer contains general restrictions and is at the top of this hierarchy. It contains two requirements: first, there should be what is termed an adequacy decision; and, second, appropriate safeguards should be applied (the first of these two requirements takes precedence over the second).

Therefore, transfer of data to a third country which has an adequacy decision from the EU Commission holds the first rank in the overall hierarchy of grounds for permitting cross-border data transfer.[27] An adequacy decision in favor of a country means that the EU Commission, after scru-

[22] Ibid. Art. 2.

[23] Ibid. Art. 45.

[24] Ibid. Art. 45–47.

[25] Ibid. Art. 49.

[26] Ibid. Art. 44.

[27] Ibid. Art. 45.

tinizing a country's legislation concerning data protection, has concluded that the regulations adopted in that country offer the same level of commitment to data protection as that established within the EEA.[28] As the EU Commission has noted, if an adequacy decision is in place with respect to certain country, then data transfer to that country does not require any further safeguard.[29] In practice, however, reliance on adequacy decisions has several drawbacks (especially for arbitration).

First, adequacy decisions have at present been issued to relatively few countries,[30] which means coverage by adequacy decisions may often be incomplete when many jurisdictions are involved in data exchange. As already mentioned, arbitration often involves various jurisdictions in which data may be transmitted in the course of arbitration proceedings, and it may be difficult (if not impossible) to create an environment fully covered by adequacy decisions.

Second, having an adequacy decision is not a permanent guarantee: in fact, even after an adequacy decision in favor of a certain country has been made, that decision may be rescinded if the actual operation of its data protection system is found to be unsatisfactory.[31] One of the most striking examples of reconsideration of data transfer regimes based on adequacy decisions is in a series of cases recently considered by the Court of Justice of the European Union (hereinafter CJEU) pertaining to invalidation of the data protection regimes agreed to between the EU and the USA (i.e. the U.S.-EU Safe Harbor Framework and the EU-US Privacy Shield regime).[32]

---

[28] Handbook on European Data Protection Law,,.European Union Agency for Fundamental Rights and Council of Europe. Luxembourg, 2018 (hereinafter Handbook on European Data Protection Law), p. 254.

[29] EU Commission website. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed: 14.04.2021)

[30] The list of the countries that have adequacy decisions is available on the EU Commission website and includes: Andorra, Argentina, Canada (as concerns commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay. Available at: *https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en* (accessed: 04.05.2021)

It should be noted separately that until 16 July 2020 the adequacy decision regulating transfer of data between the EU and the USA was in effect (although it had limited scope). Available at: https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en (accessed: 04.05.2021)

[31] Handbook on European Data Protection Law, p. 189.

[32] For more details see the press release of the EU Commission, "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield".

The first case (*Maximilian Schrems* v *Data Protection Commissioner* {"Schrems I"]),[33] was considered before the GDPR had been issued. Nevertheless, analysis of adequacy decisions provided there may also be relevant to post-GDPR practice. In this decision the CJEU invalidated the EU-US Safe Harbor regime,[34] and proclaimed that:

> [A] decision…by which the Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State,…, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.[35]

This decision had a far-reaching impact and led to a revision of data security standards between the EU and the USA. In particular, the EU-US Safe Harbor regime was reconsidered [Graham N., Mehta T., 2015] and replaced by the EU-US Privacy Shield.[36]

The second case (*Data Protection Commissioner* v *Facebook Ireland Limited and Maximillian Schrems* ["Schrems II"])[37] resulted in the invalidation of the EU-US Privacy Shield specifically because USA domestic law granted rights of access to private data for USA public authorities; this meant that the necessary data protection could not be ensured.[38] The EU

Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216 (accessed: 22.04.2021); and the press release of the Court of Justice of the European Union, No 91/20. 16.07.2020. Available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf (accessed: 22.04.2021)

[33] See the Judgment of the CJEU (Grand Chamber) of dated 06.10.October 2015 in Case C362/14 (hereinafter Case C-362/14).

[34] In accordance with the "safe harbor" regime, US companies were able to self-certify their compliance with the agreed data protection requirements, which would simplify transfer of data from the EEA to those companies (See: EU Commission Memo/00/47 dated 27 July 2000. How will the 'safe harbor' arrangement for personal data transfers to the US work? Available at: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_00_47 (accessed: 04.05.2021)

[35] See Case C-362/14, para 66.

[36] EU Commission press release. EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield. 02.02.2016. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216 (accessed: 04.05.2021)

[37] See Judgment of the CJEU (Grand Chamber) of 16. July 2020 in Case C-311/18 (hereinafter Case C-311/18).

[38] See Case C311/18, para 185.

and USA have recently been in negotiations concerning a new regulatory regime which would be more in line with the principles and standards of the GDPR.[39] Until such a regulatory regime is agreed upon, companies may consider resorting to various other grounds for the transfer of data between the EU and USA, insofar as such grounds are available to them.

These cases demonstrate that adequacy decisions cannot be considered as an entirely stable ground for cross-border data transfer (the EU-US Privacy Shield was in effect for only four years before it was also invalidated); and even if adequacy decisions are in place, they can hardly be relied upon in isolation from the actual data protection measures operating in a particular country.

For the purpose of arbitration, both the poor geographical coverage of data protection decisions and the risk of a change in the status of an adequacy decision make this tool practically useless in international arbitration and force the parties to continue making their own analysis of the data protection issues in each case.

According to Art. 46 of the GDPR, transfer of data to a third country is allowed subject to the existence of "appropriate safeguards", including enforceable rights and legal remedies for the data subject.[40] The appropriate safeguards are specifically defined by the GDPR in a list that contains such instruments as binding corporate rules,[41] standard data protection clauses[42] and approved codes of conduct.[43] When applying these principles to justify data transfer in arbitration, it is important to keep in mind at least two specific features attached to these instruments.

First, almost no deviations from the established scope of commitments imposed on the entity that is handling data are allowed, as this scope is set by the EU Commission or supervisory authority acting in each EEA country.[44] The commitments established by these instruments may be regarded as

[39] See Joint Press Statement by European Commissioner for Justice Didier Reynders and US. Secretary of Commerce Gina Raimondo. 25 March 2021. Available at: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443 (accessed: 21.04.2021)

[40] See Art. 46 and Recital 108 of the GDPR.

[41] Ibid. Art. 46 (2)(b) .

[42] In accordance with the provisions of the GDPR (Art. 46 (2)(c) and (d) of the GDPR) data controllers can choose between standard data protection clauses or "ad hoc" data protection clauses. If ad hoc clauses are to be applied, they should be specifically approved by a competent authority.

[43] Ibid. Art. 46(2)(e).

[44] See Art. 46 (2)(a) of the GDPR.

burdensome for the party receiving data[45] and inconvenient for international arbitration, especially in cases where the data recipient's "interaction" with data does not constitute a long-term established practice, but is instead the result of being involved in a particular case (e.g. as an arbitrator dealing with documents provided by the parties). A similar approach and analogous difficulties are also typical of the other types of appropriate safeguards.

Second, each instance of application of any of the appropriate safeguards requires a separate approval procedure,[46] which significantly complicates the overall compliance process and also leaves parties with almost no flexibility to arrive at terms that they are comfortable with themselves. Although employing these appropriate safeguards may seem a good solution for international arbitration at first sight,[47] their detailed provisions, which are almost completely fixed, make this ground for cross-border data transfer difficult to employ [Rosenthal D., 2019: 830].

Application of derogations allowing data transfer in international arbitration

Overview of derogations

In a situation when neither adequacy decisions nor appropriate safeguards can be applied, grounds from the second group (i.e. specific derogations) are to be considered for cross-border data transfer. The list of derogations is provided by Art. 49 of the GDPR, and it describes exceptional situations in which data transfer is allowed without either an adequacy decision or appropriate safeguards being in place. In effect, derogations are next in line under the previously mentioned cascade principle for applying grounds. The cascade principle presupposes the superiority of adequacy decisions and appropriate safeguards over specific derogations.[48]

An important consideration here is that, although application of Art. 49 of the GDPR allows cross-border transfer of data in exceptional situations, it does not negate the general obligation of a transferring party to comply with

[45] Detailed obligations are provided in 2021/914: Commission Implementing Decision (EU) of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

[46] See Art. 40, 42 and 47 of the GDPR.

[47] The European Data Protection Board Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 25 May 2018 (hereinafter Guidelines on derogations), pp. 3-4.

[48] Art. 49(1) of the GDPR.

other requirements of the GDPR.[49] In particular, Art. 44 as well as Recital 101 of the GDPR stipulate that international data transfer is to be conducted "subject to the other provisions" of the GDPR and, what is even more important, require that "the level of protection of natural persons …should not be undermined".[50]

In contrast with data transfer performed under adequacy decisions or appropriate safeguards, resort to derogations is legitimate only if data transfer takes place occasionally and does not constitute a stable channel for data transmission.[51] This peculiarity makes derogations difficult to rely on in the ordinary course of international business; however, for international arbitration this requirement is normally met. Even if company is a frequent participant in arbitration or if these rules are applied to arbitral institutions (which constantly deal with data exchanged between parties and tribunals), each particular transfer of data within arbitration occurs on an ad hoc basis and can scarcely be regarded as continuous data transmission between the entities (be they the disputing parties, the arbitrators or the arbitral institution).

The list of available derogations is closed and includes the following situations that permit cross-border data transfer:[52]

there is explicit consent to the proposed transfer;

the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

the transfer is necessary for important reasons of public interest;

the transfer is necessary for the establishment, exercise or defense of legal claims;

the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

---

[49] Guidelines on derogations, p. 3.

[50] Recital 101 of the GDPR. A similar passage is in Art. 44 of the GDPR.

[51] This requirement comes from the literal interpretation of the Recital 111 of the GDPR, which specifies that data transfer under derogations is possible *"…where the transfer is occasional…"*

[52] Art. 49(1)(a)-(g) of the GDPR.

the transfer is made from a register which is publicly available or available to persons who can demonstrate legitimate interest in consulting it;

the transfer serves the legitimate interests of the transferring party

It is apparent that not all of the derogations listed above are applicable in principle to arbitration; however, some of them may seem to be particularly suitable for it. In particular, if cross-border data transfer is required within international arbitration proceedings, the following derogations may be pertinent: having explicit consent; data transfer necessary for the establishment, exercise or defense of legal claims; or data transfer based on legitimate interest [Paisley K., 2018: 881]. Each of these grounds has its own distinctive features, and they should be considered separately.

Application of the explicit consent derogation in arbitration

Because arbitration is by nature a consensual procedure, the explicit consent derogation provided by the GDPR may seem the most logical solution, but reliance on this ground in international arbitration may be difficult in practice. The chief difficulties in resorting to this derogation arise from the GDPR requirements themselves.

The general requirements for what constitutes a data subject's consent and how it should be obtained in order to comply with the GDPR are established by Art. 4(11) and Art. 7 of the GDPR, as well as by clarifications in Recitals 32, 42 and 43 of the GDPR. In accordance with these rules data subject consent is to be freely given, specific, informed, and unambiguous.

Compliance with these requirements in the context of arbitration will have its own peculiarities. In particular, arbitration may be concerned with different types of data (sometimes even in the course of a single proceeding or one cycle of data exchange). It may involve data about employees, contractors, customers, partners, etc. [Paisley K., 2018: 870]; and in each case compliance with the GDPR principles will require different actions.

To cite one example, the transfer of an employee's data within arbitration proceedings (which is presumably the most frequent kind of data processed by the parties) may diverge from as many as three of the four requirements established by the GDPR. It may be difficult to ensure sufficient specificity[53]

[53] In particular, Recital 39 of the GDPR states that the "specific purpose should be explicit… and determined at the time of the collection of the personal data". Therefore, it is questionable whether general language regarding possible data transfer for the purposes of arbitration will be sufficient to ensure compliance.

and also compliance with the requirement of informed consent (especially when it comes to the analysis of consents obtained preemptively).[54] In particular, a conflict may arise between the level of detail required for an appropriate consent and the expected level of confidentiality in arbitration. It is also important to note that the GDPR requires that the data subject be "informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards",[55] which means that at the time when consent is received there should at least be an understanding regarding the scope of data importing jurisdictions.[56] Needless to say, this requirement is difficult to comply with until the arbitration has commenced. At the same time, if data subject consent is obtained on a case-by-case basis through a separate statement referring to a specific dispute or even to a specific operation occurring in the course of proceedings, which would probably better meet the GDPR requirements, the principle of confidentiality of arbitration may be compromised [Paisley K., 2018: 908].

Furthermore, there may be an "imbalance of power" between the employer and employee[57] that comes into conflict with the GDPR requirement of "freely given consent"[58] (e.g. the quality of consent may hinge on whether an employee actually has an option to reject a clause in the agreement).[59] Another important consideration is that establishing the data subject's consent as freely given in complex proceedings where each operation constitutes a separate act of data processing (e.g. submission of documents, consideration of witness statements, exchange of positions between the parties, writing an award etc.) [Paisley K., 2018: 845-846) requires that

---

As another example, the issue of specificity was taken up by the Commission Nationale de l'Informatique et des Libertés (CNIL), which is the French data protection authority. Its decision dated 21 January 2019 levied a fine of €50 million against Google LLC. One of the violations that Google was accused of was a lack of valid consent to data processing. In particular, the CNIL maintained that in order to consent to the privacy policy users had to give their consent not for specific purposes, but for all the processing operations. The CNIL position was that such consent was "neither specific nor unambiguous". Available at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (accessed: 15.04.2021)

[54] The European Data Protection Board Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1. dated 04 May 2020 (hereinafter Guidelines on consent), p. 7.

[55] Art. 49(1)(a) of the GDPR.

[56] Guidelines on consent, p.8.

[57] Ibid. P. 9.

[58] Ibid. P. 7.

[59] Article 29 of Data Protection Working Party, Opinion 2/2017 on data processing at work. 8 June 2017, para 6.2, p. 23.

the data subject have the option to consent to each operation separately or only to some subset of operations.[60]

Application of this rule in arbitration will mean literally that a data subject (who is normally not a party to arbitration but an employee of a party as in our example) should be provided both with information about each step of the arbitration proceedings and also should have a certain degree of influence over the procedure itself, which may lead to interference with such basic arbitration concepts as confidentiality and autonomy of the parties [Lew J.,, Mistelis L., Kroll M., 2003: 523].

This is just one specific example to show that resorting to the derogation based on the data subject's consent is a more complex matter than it might initially seem.

Furthermore, the stipulation in Article 7 of the GDPR that any consent given should be revocable at any time and that the data subject is to have the option to withdraw their consent in a manner which is as easy as giving consent is important. Thus, it follows from the GDPR's conditions for obtaining a data subject's consent and using it (and the same conclusion has been emphasized by the European Data Protection Board) that properly obtained consent gives the data subject full control over the way their date is processed and even over whether it can be processed.[61] Although this approach is reasonable in the context of data protection, it may obstruct efficient resolution of a dispute when it is applied to international arbitration.

Finally, because the data subject's consent is regarded as an exceptional rather than a standard ground for cross-border data transfer, there is a presumption of heightened risk hanging over the data subject due to the lack of adequate (i.e. analogous to the GDPR) protections.[62] In these circumstances the GDPR sets an even higher standard for the data subject's awareness of potential risk, which is why consent to cross-border data transfer must be "explicit".[63] This requirement presupposes expression of consent in a much clearer form, which also implies that more details concerning data processing operations are to be provided to the data subject.[64]

Compliance with these requirements is essential to ensure that cross-border data transfer based on the data subject's consent is lawful, and fail-

[60] Recital 32 of the GDPR.

[61] Guidelines on consent, p. 5.

[62] Ibid., p. 20.

[63] Art. 49(1)(a) of the GDPR.

[64] Guidelines on consent, p. 20.

ure to meet the requirements will incur a challenge to data transfer and significant fines.[65] Therefore, if a party chooses to collect the data subjects' consents for transfer of their data outside the EEA, that party should make sure that the standards set by the GDPR are accurately met. This exercise is not easy in itself, and it becomes even more difficult for arbitration, as the requirements of the GDPR may come into conflict with the requirements and basic concepts that are peculiar to international arbitration.

Application of the legal claims derogation

One more ground for cross-border data transfer which may be employed for the arbitration is provided by Art. 49(1)(e) of the GDPR. This provision states that transfer outside the EEA is allowed when "…necessary for the establishment, exercise or defence of legal claims". Recital 111 of the GDPR further clarifies that the legal claims derogation covers a wide range of proceedings, "whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies." The term "out-of-court procedure" implies that the legal claims derogation may also cover arbitration [Paisley K., 2018: 880].

Nevertheless, a party applying this derogation should take into account that, in accordance with Art. 49(1)(e) of the GDPR, the lawfulness of cross-border data transfer in these cases will depend upon whether the data transfer is actually "necessary" — i.e. there must be compliance with what is termed the "necessity test".[66] This test requires analysis of the data in question and of its relevance to the specific legal proceedings,[67] and thus it coheres with major principles of data protection that have been established elsewhere in the GDPR such as "purpose limitation"[68] and "data minimization".[69]

Application of the necessity test has several implications in practice. In particular, it restrains the data controller (which may be a party to a dispute

[65] In accordance with Art. 83(5)(a) of the GDPR, the fine for a breach of "the basic principles for processing, including conditions for consent…" may be up to €20,000,000 EUR or up to 4 % of the total worldwide annual turnover of the breaching entity for the preceding financial year.

[66] If Art. 49(1) of the GDPR is interpreted literally, the legal claims derogation would not be the only one subject to the necessity test. The same language is also used for the derogations provided by Articles 49(1)(b), (c), (d) and (f). (See Guidelines on derogations, p. 12).

[67] Ibid., p. 12.

[68] Art. 5(1)(b) of the GDPR.

[69] Ibid. Art. 5(1)(c).

submitted for arbitration) from transferring all the data that is potentially relevant to the legal proceedings[70] and requires limiting that data to what is directly related to the proceedings.[71] Depending on the stage in the arbitration proceedings, compliance with this rule may be challenging. When certain data, or a document containing that data, is specifically requested from a party, its relevance and necessity may be relatively easy to verify. However, when the data is included in a memorandum or any other procedural document introduced by a party voluntarily, it may require a more careful and detailed explanation of the usage of the data in question.

There are many practical recommendations that can help the transferring party in complying with these rules (for instance, the party might consider the feasibility of transferring anonymized or pseudonymized data, etc.).[72] But it is important in any case for the transferring party to understand that applying this ground will mean managing both the risk of noncompliance with the GDPR requirements (if the party fails to confirm the relevance or necessity of the transferred data to a particular dispute) and also the risk of providing insufficient evidence to succeed in arbitration (if the party takes a conservative position concerning amount of data to transfer).

This allocation of risks (or more precisely, assigning all risks to the transferring party) reveals another interesting peculiarity when the GDPR is applied to international arbitration. For example, a regulatory framework for arbitration may allow document production in principle [Born G., 2015: 186], while the decision on the relevance and necessity of certain documents will be taken by the tribunal (although with due consideration of positions of the parties).[73] A decision by the tribunal may contradict the party's evaluation of the same matter and present the party with the

[70] Guidelines on derogations, p. 12.

[71] This principle is also highlighted by Article 29 Data Protection Working Party, Working Document 1/2009 on pre-trial discovery for cross border civil Litigation. 11 February 2009, p.10.

[72] Guidelines on derogations, p. 12.

[73] For example, Art. 3(7) of the International Bar Association Rules on Taking Evidence in International Arbitration (as adopted by a resolution of the IBA Council 29 May 2010), provides: "The Arbitral Tribunal may order the Party to whom such Request is addressed to produce any requested Document in its possession…". A similar approach is followed by Art. 27(4) of the UNCITRAL Arbitration Rules (as revised in 2010) establishing that "the arbitral tribunal shall determine the admissibility, relevance, materiality and weight of the evidence offered"; as well as by the majority of arbitration rules (see for example: Art. 19.2 of SIAC Rules 2016; Art. 22.2 of HKIAC Rules 2018, Art. R-34(b) of AAA Commercial Arbitration Rules and Mediation Procedures, etc.).

difficult choice of which requirements to comply with. Furthermore, the GDPR in Art. 48 establishes separate rules for transferring data in response to foreign judgements or decisions. This dichotomy within the GDPR itself points to another important issue that affects the legitimacy of cross-border data transfer: the interplay between Art. 48 of the GDPR, and the legal claims derogation.

Interplay between Art. 48 of the GDPR and the legal claims derogation

Art. 48 of the GDPR refers to situations in which transfers or disclosures are not authorized by EU law. Parties should refrain from transferring data in response to a court judgment or decision of a third country if the judgement or decision requiring data transfer is not "based on an international agreement…between the requesting third country and the Union or a Member State". Art. 48 of the GDPR broadly characterizes the bodies that may issue such judgements as courts, *tribunals* and administrative authorities. This makes Art. 48 analogous to Art. 49(1)(e) of the GDPR, as it also would extend to arbitration.

Art. 48 would then provide an answer the question about appropriate grounds for data transfer by specifying that the transfer is to be requested by a competent authority (which would be an arbitral tribunal for the purpose of this article) as well as outlining the requirements to be followed in these matters.

The explication of GDPR Art. 48 provided in the "Guidelines on derogations" states that requests for data transfer from bodies of the types permitted (for our purpose, arbitral tribunals) are not "in themselves legitimate grounds for data transfers".[74] Whether cross-border data transfer in these cases is permissible depends on two factors: first, there must be an international agreement between the two countries (the country of the authority making the request and the country of the party making a disclosure); and second, there must be a level of data protection consistent with the GDPR.[75]

In practice Art. 48 of the GDPR may provide the transferring party with two options for responding to a judgement or decision requiring data transfer outside the EEA depending on whether or not there is an agreement between the countries in question:

[74] Guidelines on derogations, p. 5.

[75] See Recital 115 of the GDPR.

if there is an agreement between the European Union or the corresponding member state and the country of the requesting authority, refer the authority making the request to the procedure for international cooperation established by that agreement (e.g., mutual legal assistance treaties);[76]

if there is no such agreement, find other grounds to justify data transfer among those that are offered by the GDPR, usually in Art. 49.[77]

This solution follows from the official guidelines on GDPR application[78] and comes from Art. 48, which stipulates that it is to be applied "without prejudice to other grounds for transfer". However, on closer examination and especially in employing this solution for arbitration, a number of questions arise.

First, it is well-known that international agreements on legal assistance between states do not common for arbitration [Paisley K., 2018: 875]. That lack may make it difficult to ascertain whether Art. 48 of the GDPR will be useful in arbitration (at least until appropriate international agreements between states come into play). However, even if we suppose that there are bilateral or multilateral treaties as envisaged by Art. 48 that pertain to arbitration, that will not automatically settle the issues in applying Art. 48. At a bare minimum, there would still be the question of how to determine the nationality of an arbitration proceeding, as this may be important in understanding which specific international agreement to apply. For national courts and for administrative or investigative authorities, the jurisdictional link is immediately apparent; but for international arbitration the boundaries are blurred. This has become quite evident with the advent of the concept of delocalized arbitration, which presupposes that international arbitration is detached from any national legal system [Lew J., 2006: 179–204].

Although one possible solution could be reliance on the seat of the arbitration[79] by analogy with the approach most commonly taken to determine the nationality of an award under New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards (hereinafter New York

[76] Guidelines on derogations, p. 5.

[77] See Recital 115 of the GDPR; Guidelines on derogations, p.5.

[78] Guidelines on derogations, p. 5.

[79] It should be noted that even for purposes of enforcement, the seat of arbitration is not the only possible criterion. For instance, the wording in Art. I (1) of the New York Convention, suggests that the convention should be applied to "…arbitral awards made in the territory of a State other than the State where the recognition and enforcement of such awards are sought....", as well as to "arbitral awards not considered as domestic awards in the State where their recognition and enforcement are sought."

Convention) [Lew J., Mistelis L., Kroll M., 2003: 700], this approach hardly seems compatible with the key purpose of data protection regulation, which is to defend data subjects' rights from possible negative influence by the regulatory environment in the country to which the data is actually transmitted.[80] This purpose has little or no relevance to the seat of arbitration. It should instead entail consideration of the national laws applicable to entities receiving the data (arbitrators, opposing parties, arbitral institution, etc.). In practice this means that the application of data security standards and grounds for data transmission in arbitration may be extremely fragmented.

A second problem with the approach to application of Art. 48 of the GDPR suggested above is that it assumes in effect that the limitations of Art. 48 can always be overridden by the GDPR's other provisions (such as the derogations offered by Art. 49). This is specifically pertinent to arbitration because there are often no international agreements to apply. The presumption would then be that it is always possible to find alternative grounds to justify cross-border data transfer.

That regulatory strategy does not seem very logical because there is no clear reason for imposing a restriction that can be easily ignored by applying another clause of the same regulation. We could perhaps use the "cascade principle" described earlier to settle this problem as well; however, that suggestion does not fully align with the general logic of the GDPR. We can think of several reasons that explain why adequacy decisions take precedence over, say, the derogations that may be available. From the perspective of a regulator, adequacy decisions should be the first recourse because the regulator will have been able to verify the security of data transmission in advance. The data transferring party should also see this approach as acceptable because adequacy decisions release them from complying with the more complex and burdensome requirements of the GDPR. However, neither of these lines of thinking can provide a definitive answer to the question concerning the relationship between Articles 48 and 49 of the GDPR. Until further explanations are provided by the regulatory authorities of the EU, the confusion will continue and leave the transferring party to wrestle with whether they can use other available grounds for the transfer of data (such as those provided by Art. 49) or should instead completely refuse the transfer.

Refusing transfer would be consistent with a more conservative opinion about application of Art. 48. According to that position, Art. 48 may be

[80] See Communication to the EU Parliament.

viewed as restricting reliance on Art. 49(1)(e) of the GDPR only to legal claims pursuant to judgements or decisions which are in turn supported by international bilateral or multilateral agreements.[81] If this interpretation holds (again provided that there are no international agreements that apply to international arbitration), then cross-border data transfer in arbitration would be paralyzed in many ways because the legal claims derogation, which is currently the most suitable ground for transfer of data in international arbitration, would become difficult or almost impossible to apply.

The plain language of Art. 48 of the GDPR also suggests that an international agreement is required in order to *enforce or recognize* a decision or judgment on data transfer to a third country rather than to substitute for or supplement the other grounds for cross-border data transfer provided by the GDPR. As further clarified by Recital 115 of the GDPR, the purpose of this limitation is to preclude extraterritorial application of "laws, regulations and other legal acts" of third countries, which may require data transfer but not provide data protection analogous to that required by the GDPR.[82]

Such a literal interpretation of the GDPR's provisions may suggest a third possibility for applying Art. 48 by maintaining that voluntary compliance with judgements and decisions on data transfer (when no enforcement procedures are involved) falls outside the scope of Art. 48, which would then be applicable only in the event that enforcement of a judgement or decision is required. However, following this interpretation for arbitration proceedings is questionable because even when data transfer is ordered by a tribunal (e.g. as a part of production of evidence), that order has limited potential for enforcement. The main incentive to comply with the order would be to avoid adverse inferences that would be prejudicial to a party that refuses to comply with a disclosure order.

As things currently stand, application of Art. 48 of the GDPR in international arbitration is complicated by a number of factors, including lack of clarity about the exact circumstances in which it should be applied and lack of appropriate international treaties designed for international arbitration as well as the limited enforcement capacity of the tribunals' orders. This

[81] See the report by Ernst & Young. Practical considerations for cross-border discovery under the General Data Protection Regulation (GDPR). Available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-forensics-e-discovery-practical-considerations-for-cross-border-discovery-under-gdpr.pdf (accessed: 14.04.2021)

[82] Recital 11 of the GDPR.

lack of clarity also brings into question the proper application and pertinence of Art. 49(1)(e) of the GDPR for international arbitration.

Application of the legitimate interest derogation

The last resort for a derogation that permits data transfer in international arbitration when none of the previously described grounds and derogations can be applied is provided by Art. 49(1)§2 of the GDPR (i.e. the legitimate interest derogation).[83] In practice, this provision may be invoked, if not all the data that party is willing to transfer falls under the legal claims derogation (e.g. it may be difficult to establish direct relevance between the data in question and the arbitration proceedings) [Paisley K., 2018: 876].

In order to comply with Art. 49(1)§2 of the GDPR, the disclosing party should ensure compliance with the following conditions:

data transfer is not repetitive;

only a limited number of data subjects is concerned;

data transfer is necessary for the purposes of "compelling legitimate interests pursued by the controller" and such interests "are not overridden by the interests or rights and freedoms of the data subject";

the controller has assessed all the circumstances surrounding the data transfer and has used that assessment to introduce suitable safeguards for protecting personal data.

In addition to compliance with those requirements, a data controller relying on the legitimate interest derogation should also notify the supervisory authority of the transfer.[84]

A comparison of this provision with Art. 49(1)(e) of the GDPR (the legal claims derogation) points up at least two complications peculiar to the legitimate interest derogation: first, the requirement to notify the supervisory authority during international arbitration could involve a breach of confidentiality; and second, there is a higher threshold for the necessity test that transferring party must meet.[85]

In particular, the disclosing party resorting to Art. 49(1)§2 of the GDPR should be able not only to substantiate that the transfer is necessary, but also to demonstrate that this necessity is derived from "compelling legitimate

[83] Guidelines on derogations, p. 14.

[84] See §3 of Art. 49(1) of the GDPR.

[85] Guidelines on derogations, p. 12.

interests". There is no direct answer at the moment about whether transfer of data for the purpose of participating in arbitration should be considered as a compelling legitimate interest or not. But the example suggested by the European Data Protection Board in this matter suggests that, in order to comply with the established standard, the disclosing party should be able to demonstrate that transfer of data was required as a protection "from serious immediate harm or from a severe penalty which would seriously affect…business".[86]

It follows that this ground may be applied in arbitration depending on the factual circumstances in arbitration that frame the cross-border data transfer and on the potential negative consequences incurred by failing to transfer. However, the issue of notification remains a substantial obstacle to ready reliance on this ground because confidentiality is a basic principle of arbitration, as has previously been mentioned.

The foregoing analysis shows that all of the grounds on which a party can rely for justifying cross-border data transfer provide almost no solution that would suit international arbitration. Even resort to the legal claims and legitimate interest derogations does not provide the transferring party with full protection from claims and challenges related to non-compliance or improper compliance with the GDPR requirements; and, equally important, neither of those rules take into account such distinctive features of arbitration as the requirement of confidentiality or the predominantly voluntary nature of arbitration.

Conclusion

International arbitration is now faced with data protection requirements (and in particular the GDPR) that allow nearly no acceptable or risk-free solutions, which would enable parties to meet all of the necessary requirements. This is because the requirements have been formulated without taking into account industry specifics (for our purposes, the specific rules and principles that distinguish international arbitration from other types of procedures for dispute resolution).[87] Therefore, the incentive to comply may be significantly reduced, and diligent compliance may be supplanted by a formalistic exercise.

[86] Ibid., p. 15.

[87] It should be noted that some jurisdictions, e.g. the USA, historically follow "more of a fragmented and sector-specific approach" [Cooper D., Kuner C., 2017: 48]. Nevertheless, expansion of the digital environment and the huge increase in electronic data exchange largely blurs the differences in regulatory approaches.

Although the specific requirements may differ from jurisdiction to jurisdiction, it would be fair to say that regulators increasingly tend to gravitate toward a more stringent rather than a more relaxed approach to data protection (especially in the context of the cross-border data exchange). For instance, Russian regulation (which, along with the Chinese one, is frequently cited as a major antagonist to the GDPR) does not recognize legal claims derogation to legitimate cross-border data transfer and relies primarily on the data subject's consent or adequacy decisions.[88] Some jurisdictions also apply so-called "blocking statutes" that literally prohibit the transfer of data to foreign jurisdictions and apply criminal penalties to it.[89] Instances of data protection regulations that are nuanced and adaptive are very rare, if not completely absent.

As data protection regulations penetrate almost every aspect of life and business, companies covered by those regulations become more inclined to "tick the right boxes" and find the most convenient ways to justify their practices rather than to protect the real interests of data subjects with due consideration of all relevant circumstances. This outcome has strayed far from the initial ideas that prompted data protection regulation and probably neglects the interests of private data subjects themselves.

In order to overcome this problem and to develop regulations which would be helpful in achieving the important task of private data protection, it is necessary to carefully consider all the industries and sectors that may

[88] In accordance with Art. 12 of the Federal Law of the Russian Federation "On personal data" No 152-FZ 27.07.2006, cross-border data transfer is allowed only subject to the following limited set of conditions: the country to which the data is to be transferred provides adequate protection of personal data (such protection may be ensured either by the fact of being signatory to the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, or by being added to a separate list of states with adequate data protections); the data subject has provided his/her written consent; the data transfer is provided for by an international treaty; the data transfer is provided for by the relevant federal laws and is necessary to protect the Constitution, to ensure the country's defense and state security, as well as to ensure the security of the stable and safe functioning of the transport system; the data transfer is required to execute a contract to which the data subject is a party; the data transfer is necessary to protect the data subject's rights and interests.

[89] 00339/09/EN WP 158: Working Document 1/2009 on pre-trial discovery for cross border civil litigation. 11 February 2009, p. 5. See for example, the French Statute № 68-678 of 26 July 1968, modified by the French Statute No 80-538 of 16 July 1980; the Swiss Criminal Code; China State Secrecy Law; Australian Foreign Proceedings (Prohibition of Certain Evidence) Act 1979, etc. (for more details seethe Sedona Conference Framework for Analysis of Cross-Border Discovery Conflicts: a practical guide to navigating the competing currents of International Data Privacy and e-Discovery, 2008 Public Comment Version, 2008 the Sedona Conference, pp. 18–20).

be affected by the data protection regulations and make sure that any such regulation is organically embedded into the existing ecosystems without unnecessarily subverting the principles peculiar to each of them. Building an effective defense for privacy should be the primary purpose.

One possible solution that should be considered in order to reduce the current fragmentation (at least in matters of cross-border transfers) would be to arrive at suitable international conventions that would balance the regulatory concerns of different countries and provide all the stakeholders with greater predictability in data protection requirements.

References

Born G. (2021) *International Commercial Arbitration*. 3rd ed. The Hague: Kluwer Law International, 4250 p.

Born G. (2014) *International Commercial Arbitration*. 2nd ed. The Hague: Kluwer Law International, 4000 p.

Burianski M., Reindl M. (2010) Truth or dare? The conflict between e-discovery in international arbitration and German data protection rules. *Schieds VZ: German Arbitration Journal,* no 4, pp. 182–200.

Cohen S. Morril M. (2017) A call to cyberarms: The international arbitrator's duty to avoid digital intrusion. *Fordham International Law Journal*, no 3, pp. 957–1005.

Cooper D., Kuner C. (2017) Data Protection Law and International Dispute Resolution. In: Collected Courses of the Hague Academy of International Law, vol. 382 Leiden/Boston: Hague Academy of International Law, pp. 9–174.

Graham N., Mehta T. (2015) Safe Harbor in a storm: ECJ rules on data transfers to the US. *Practical Law UK*. Articles 3-619-7150. Available at: https://uk.practicallaw.thomsonreuters.com/3-619-7150?contextData=(sc.Default)&transitionType=Default&firstPage=true (accessed: 20.04.2021)

Kuner C. (2013) *Transborder Data Flows and Data Privacy.* Oxford: University Press, 285 p.

Lew J., Mistelis L., Kroll M. (2003) *Comparative International Commercial Arbitration*. The Hague: Kluwer Law International, 953 p.

Lew J. (2006) Achieving the dream: Autonomous arbitration. *Arbitration International,* no 2, pp. 79–204.

Maldoff G. (2016) White Paper, CIPP/US, IAPP Westin Fellow. The risk-based approach in the GDPR: Interpretation and implications. Available at: https://iapp.org/resources/article/the-risk-based-approach-in-the-gdpr-interpretation-and-implications/ (accessed: 20.04.2021)

Paisley K. (2018) It's all about the data: The impact of the EU General Data Protection Regulation on international arbitration. *Fordham International Law Journal*, no 4, pp. 854–908.

Pastore J. (2017) Practical approaches to cybersecurity in arbitration. *Fordham International Law Journal*, no 3, pp. 1023–1029.

Rosenthal D. (2019) Complying with the General Data Protection Regulation (GDPR) in international arbitration — Practical guidance. *Association Suisse de l'Arbitrage Bulletin*, no 4, pp. 822–852.

Schwarz E. (2018) Ernst & Young report. Practical considerations for cross-border discovery under the General Data Protection Regulation (GDPR). Available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-forensics-e-discovery-practical-consideration сц3у смма4ку4 s-for-cross-border-discovery-under-gdpr.pdf (accessed: 20.04.2021)

Smeureanu I. (2011) Confidentiality in International Commercial Arbitration. International Arbitration Law Library. Vol. 22. The Hague: Kluwer Law International, 232 p.

Tschanz P.-Y. (2006) Switzerland: Confidentiality of Swiss Supreme Court review of arbitral awards. Available at: https://www.mondaq.com/Litigation-Mediation-Arbitration/43062/Confidentiality-Of-Swiss-Supreme-Court-Review-Of-Arbitral-Awards (accessed: 20.04.2021)

Warren S., Brandeis L. (1890) The right to privacy. *Harvard Law Review*, no 5, pp. 193–220.