

Data Privacy Concerns in Virtual ADR Sessions

PhD. student **Andrada-Laura TARMIGAN**¹

Abstract

The aim of this article is to analyze the data privacy issues related to the technology used in hybrid and virtual alternative dispute resolution (“ADR”) procedures, in accordance with the General Data Protection Regulation (“GDPR”) and generally imposed standard at an international level. The results are obtained through the comparative method and are relevant in identifying the rights and obligations of all stakeholders: the supervising institutions, decision makers, the parties and all other entities. We will analyze how leading ADR institutions position themselves in relation with data privacy issues, which is the key language involved and how are new platforms going to be prepared for the increasing volume of these speedier procedures. Lastly, we will identify potential differences between on-chain and off-chain disputes. The results are of practical importance, helping all participants in ADR procedure to understand and comply with data privacy and cybersecurity concerns,

Keywords: data privacy, cybersecurity, alternative dispute resolution, arbitration.

JEL Classification: K33

1. Introduction

Data privacy and cybersecurity have been constant matters of concern in the past years, affecting all fields of activity. Since ADR generally equals flexibility, virtual or at least hybrid meetings became the international norm, with all stakeholders having a legitimate expectancy towards it. In this context, it is necessary to consider and regulate the application and limits of data privacy norms.

Therefore, we will address the practical implications of data privacy and cybersecurity in the context of ADR proceedings, with a focus on international arbitration.

First, we will analyze different scenarios to see which law applies to data protection and more importantly, if the GDPR² applies, as mandatory law, to an arbitration seated outside the EU. Furthermore, should the parties consider these issues in the contract or leave it all in the hands of the organizing institution, where the case may be?

Secondly, we will determine if the activities related to ADR fall within the scope of the GDPR.

Thirdly, we will identify the practical steps required for all actors involved in dispute resolution procedures.

Lastly, we will discuss the cybersecurity standards in international ADR procedures.

2. Applicable Data Protection Law in arbitration and other ADR procedures

When determining if the GDPR applies to an arbitration or another ADR procedure, we shall observe its (A) territorial scope and (B) material scope.

A. Territorial scope. Art. 3 of the GDPR (“*Territorial scope*”) states that it “*applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*”

It also applies to the processing of personal data of data subjects who are in the Union by a controller³ or processor not established in the Union, where the processing activities are related to the offering of goods or services, to such data subjects in the Union or the monitoring of their behavior if it takes place within the Union.

¹ Andrada-Laura Tarmigan - Doctoral School of Law, Bucharest University of Economic Studies, andrada.tarmigan@drept.ase.ro.

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

³ Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 2021, the document is available online at https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf (last accessed 2 April 2023).

For example, a witness based in the EU may import GDPR obligations into an arbitration, even if the procedure itself is otherwise completely independent of the EU.⁴

By applying these principles to arbitration and to other types of ADR, accordingly, we will identify the actors that could fall within the territorial scope of the GDPR. Firstly, the parties to the arbitration would fulfill the above-mentioned criteria if either they are based in the EU or they are doing business and collecting data in the EU, even if they have their domicile or headquarters outside of the EU.

Secondly, arbitrators that reside in any EU member state would fall within the territorial scope of the GDPR, independently from where the institution is based. The same principles should apply to mediators, negotiators, board members in adjudication procedures etc.

In what concerns the other stakeholders to an ADR procedure, such as experts or administrative assistants, it is relevant if an institution based in the EU administers the procedure. In the case of ad-hoc arbitration, for example, the application of the territorial criteria based on the nationality or headquarters of these actors would be difficult to support.

Another important aspect would be to determine the connection between the applicable data protection regulation and the several laws that are usually involved in an international ADR procedure. For example, in the case of arbitration, we should determine if the *lex arbitri*, and substantive governing law are laws of an EU member state.

Moreover, we should consider the application of personal data regulations outside the EU. Notable examples are the UK General Data Protection Regulation⁵ or the different data privacy regulations applicable in different industries in the United States of America (health insurance, finance).

The U.S. law that is most comparable to GDPR is the California Consumer Privacy Act (CCPA⁶), which applies to consumers who are California residents.

Moreover, we have the new TADPF⁷, meant to facilitate the flow of data between the EU and the U.S., and standard contractual clauses⁸ as approved data transfer methods. The same applies for a cooperation between the EU and the UK, the UK and the US and so on.

A global perspective on Data protection reveals that states or entities with common values and interests have similar regulatory regimes. The GDPR has become a blueprint for other non-EU jurisdictions and achieved an extraterritorial level.⁹

Regardless of the applicable laws, regulatory compliance with data privacy is essential for maintaining participants' trust and avoiding substantial legal and financial consequences.¹⁰

B. Material scope. According to Article 2(1) of the GDPR, its material scope extends to all “processing of personal data wholly or partly by automated means”.

Based on this definition the parties and the tribunal in an arbitration (and similar to other ADR procedures) would process personal data, especially during document production and review. This is confirmed by another GDPR provision, which states that it was intended to apply to “out of court procedures”.¹¹

⁴ Pierre Bienvenu, Benjamin Grant, *Data protection and cyber risk issues in arbitration*, “International arbitration report”, issue 13, 2019, p. 19.

⁵ The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR), the document is available online at <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> (last accessed 2 April 2023).

⁶ The California Consumer Privacy Act of 2018, available at <https://theccpa.org/>.

⁷ Trans-Atlantic Data Privacy Framework, available at <https://www.tadpf.eu/>.

⁸ Commission Implementing Decision (EU) 2021/914 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, the document is available online at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en (last accessed 3 April 2023).

⁹ White and Case Report, *A world of clubs and fences. Changing regulation and the remaking of globalization*, the document is available online at <https://www.whitecase.com/insight-our-thinking/global-clubs-fences> (last accessed 3 April 2023).

¹⁰ Cristina Pop, *EU vs. US: What Are the Differences Between Their Data Privacy Laws?*, 2022, the document is available online at <https://www.endpointprotector.com/blog/eu-vs-us-what-are-the-differences-between-their-data-privacy-laws/> (last accessed 5 April 2023).

¹¹ Gerald Leong, *How Do You Deal With Data Protection And Cybersecurity Issues In a Procedural Order?*, Kluwer Arbitration Blog, 2020, the document is available online at <https://arbitrationblog.kluwerarbitration.com/2020/02/19/how-do-you-deal-with-data-protection-and-cybersecurity-issues-in-a-procedural-order/> (last accessed 5 April 2023).

However, some arbitral tribunals decided that the arbitration did not fall within the material scope of the GDPR, when the procedure was falling under a treaty *to which neither the European Union nor its Member States are party*¹². It is important to note that the premise is an investment arbitration and not a commercial one.

A further issue is whether the arbitral, mediation, conciliation institutions are subject to the GDPR because of their status of international organizations, that should be ensuring transparency and accountability in their operations.

Supervising institutions or, if they do not have separate legal capacity, the commercial chambers where they are established can be qualified as data controllers, from the perspective of those who determine the purpose and means of data processing.¹³ The same applies to arbitrators themselves, especially in *ad-hoc* proceedings. Arbitrators or the members of a composed decision-body could act as joint controllers, under the meaning of art. 26 of the GDPR. However, considering their degree of independence, the fact that they may have different nationality, different legal regimes, it might be preferable for them to separate themselves as individual data controllers.

Data controllers in ADR procedures should take into consideration: (i) informing the concerned data subjects about the processing, by privacy notices and privacy policies¹⁴; (ii) managing requests from data subjects¹⁵; (iii) regulating relationships with processors¹⁶ (cloud service providers, experts, translators); (iv) implementing measures for ensuring security of processed data¹⁷; (v) keeping records¹⁸.

Therefore, the GDPR does not regulate any arbitration proceedings in the abstract, but the processing activities of data controllers and processors that fall within its territorial and material scope.¹⁹

3. Legal ground for data processing in ADR procedures

Consent is not an appropriate ground for legal procedures in general, since the interested party can withdraw it at any time. However, the following alternatives from art. 6 of the GDPR are solid options: the legitimate interest, the necessity to perform a contract where one of the parties to the dispute is a natural person or, in certain cases, the legal obligation.

4. Supervision of data processing

General principles of judiciary procedures also apply to ADR procedures. The GDPR considers the risk of affecting the independence of the decision-making body and regulates the possibility to entrust the supervision of data processing to specific bodies within the Member States, which have attribution by law regarding data privacy compliance.²⁰

¹² Tennant Energy LLC v. Government of Canada, PCA Case No. 2018-54, the document is available online at <https://www.italaw.com/cases/7250> (last accessed 12 April 2023).

¹³ Martin Zahariev, *GDPR Issues in Commercial Arbitration and How to Mitigate Them*, "Kluwer Arbitration Blog", 2019, the document is available online at <https://arbitrationblog.kluwerarbitration.com/2019/09/07/gdpr-issues-in-commercial-arbitration-and-how-to-mitigate-them/> (last accessed 7 April 2023).

¹⁴ Art. 12-14 of GDPR.

¹⁵ Art. 15-22 of GDPR.

¹⁶ Art. 28 of GDPR.

¹⁷ Art. 32 GDPR.

¹⁸ Art. 30 of GDPR.

¹⁹ Emily Hay, *The Invisible Arm of GDPR in International Treaty Arbitration: Can't We Make It Go Away?*, "Kluwer Arbitration Blog", 2019, the document is available online at <https://arbitrationblog.kluwerarbitration.com/2019/08/29/the-invisible-arm-of-gdpr-in-international-treaty-arbitration-cant-we-make-it-go-away/> (last accessed 29 March 2023).

²⁰ Martin Zahariev, *Data Protection in Commercial Arbitration: In the Light of GDPR*, Lambert Academic Publishing, 2019, p. 214.

5. Application of GDPR principles in arbitration and other ADR procedures

ICCA²¹ and the IBA²² have established a joint guide on *Data Protection in International Arbitration Proceedings*, with the purpose of developing guidance to assist arbitration professionals with their data protection obligations during the specific context of arbitration proceedings.

General GDPR principles such as minimization in data collection, storage limitation and accountability apply to ADR procedures. Specific categories of sensitive data require extra protection.

Data controllers such as arbitral institutions, arbitrators, mediators, mediation institutions should consider good practices for being able to prove at any point that they are GDPR compliant. All stakeholders can receive a GDPR agreement that contains at least references to what personal data will be collected and how it will be processed, for what purposes and on what grounds, which are the main responsibilities of data controllers etc.

6. Cybersecurity and ADR procedures

ADR procedures are preferred over litigation because of their features, such as confidentiality, that is endangered in the era of virtual proceedings. It is important to note though that confidentiality does not exclude the transfer of data. The entities or persons organizing ADR procedure should adopt appropriate measures to protect electronic documents or other information against unauthorized access.²³

ADR procedures and especially high-profile arbitration cases were targets of cyberattacks²⁴. Several international institutions joined forces to launch a Working Group on Cybersecurity in Arbitration, updated in 2022 to reflect the maturing of the cybersecurity and data protection environment and now includes a data breach protocol.²⁵

The Protocol makes an important distinction between security incident and security breach, especially for enforcing the protocol for a security incident. The term “*security incident*” refers to “*an event that may have compromised the confidentiality, integrity, or availability of data or systems, such as a malware infection, loss or theft of equipment, denial of service attack, or a phishing attempt*”. A “*security breach*,” is an incident that “*results in unauthorized access to data and/or requires that notice be given to persons whose data has been compromised and/or to supervisory authorities*”.²⁶

Even if in practice we are not there yet, the etalon behavior is to provide a safe platform for document and other information exchange.²⁷ A cybersecurity strategy is another aspect that nowadays has to be considered by, in the case of arbitration, the arbitral tribunal or the supervising institution. It is debatable if it is a procedural or an administrative matter, because this would dictate if such measures should be included in the procedural orders or arbitration rules.

Moreover, all participants should give their consent towards these measures at an early stage of the procedure, if not already included in the rules of the institution.

Cybersecurity measures could be difficult to approach for those arbitrators, mediators,

²¹ The International Congress and Convention Association.

²² The International Bar Association.

²³ Claire Morel de Westgaver, *Cybersecurity in International Arbitration: Don't be the Weakest Link*, “Kluwer Arbitration Blog”, 2019, the document is available online at <https://arbitrationblog.kluwerarbitration.com/2019/02/15/cybersecurity-in-international-arbitration-dont-be-the-weakest-link/> (last accessed 8 April 2023).

²⁴ In July 2015, the website of the Permanent Court of Arbitration (PCA) was attacked by malware in the midst of an ongoing maritime border dispute between China and the Philippines.

²⁵ Cybersecurity in International Arbitration ICCA-NYC Bar-CPR Working Group, 2022, the document is available online at <https://www.arbitration-icca.org/cybersecurity-international-arbitration-icca-nyc-bar-cpr-working-group> (last accessed 12 April 2023)

²⁶ Idem, p. 8

²⁷ Bryan Cave Leighton Paisner, *International Arbitration Survey: Cybersecurity in International Arbitration*, 2018, the document is available online at <https://www.bclplaw.com/a/web/160089/Bryan-Cave-Leighton-Paisner-Arbitration-Survey-Report-2018.pdf> (last accessed 10 April 2023).

experts that come from a purely legal background. For this reason, there is an additional cost aspect to cybersecurity, covered by the parties or included in the taxes applied by the supervising institution.

Furthermore, the arbitral tribunal or a different entity in other cases should be allowed to impose sanctions for breaching cybersecurity obligations.²⁸

Clients would be willing to pay a higher fee with an arbitration institution that provided advice and assistance on appropriate security measures or provides a secure platform on which all communications and data sharing storage can take place. A recent ICC brief²⁹, that contains concrete recommendations regarding cybersecurity, shows that most arbitration users now support adopting specific measures, for example encryption, to safeguard the privacy of electronically stored data.³⁰

Lastly, we have probably the most important issues. The first one refers to the liability of parties or arbitrators that caused a security breach, either by negligence or by intent and the applicable law to determine the sanctions.³¹

Secondly, a question can be raised regarding the possibility of annulling an arbitral award that was rendered in a procedure whose security was breached. The answer resides in the direct relation between the fabricated³² or illicitly obtained data and the adopted solution.

7. Conclusion

Virtual hearings and digital information exchanges are now essential components of efficient ADR proceedings. It is important for ADR procedures to adapt in order to maintain a competitive advantage to national courts.

In ADR procedures, data protection regulations cover the processing activities of data controllers and processors that fall within its territorial and material scope.

Taking GDPR and arbitration as example, the fact that any stakeholder is subject to GDPR may potentially have implications for the other participants in the arbitration and the proceedings as a whole. This means that any data processing under ADR shall be performed in accordance with the GDPR and a failure to comply carries significant penalties.

Effective case management implies addressing data privacy issue at an early stage, for example in the case of arbitration, in the procedural order and it is recommendable for arbitrators to draft and sign agreements on the processing of personal data. Furthermore, aspects such as records of processing activities, codes of conduct, breach notifications, protocol of data transfer to third parties shall be considered.

Bibliography

1. Bryan Cave, Leighton Paisner, *International Arbitration Survey: Cybersecurity in International Arbitration*, 2018.
2. Claire Morel de Westgaver, *Cybersecurity in International Arbitration: Don't be the Weakest Link*, "Kluwer

²⁸ Claire Morel de Westgaver, *Cybersecurity In International Arbitration – A Necessity And An Opportunity For Arbitral Institutions*, "Kluwer Arbitration Blog", 2017, the document is available online at <https://arbitrationblog.kluwerarbitration.com/2017/10/06/cybersecurity/> (last accessed 12 April 2023).

²⁹ International Chamber of Commerce, *Cybersecurity Issue Brief no. 2*, the document is available online at <https://iccwbo.org/news-publications/policies-reports/icc-cybersecurity-issue-brief-2-implementing-norms-and-rules-for-responsible-state-behaviour-in-cyber-space-and-enhancing-cooperation-to-counter-cybercrime/> (last accessed 12 April 2023).

³⁰ John Choong, Vasuda Sinha, Sofia Klot, Olivier André, *Data protection and cybersecurity in international arbitration remain in the spotlight*, the document is available online at <https://www.freshfields.com/en-gb/our-thinking/campaigns/international-arbitration-in-2023/data-protection-and-cybersecurity-in-international-arbitration-remain-in-the-spotlight/> (last accessed 28 March 2023).

³¹ Erik G. W. Schäfer, *Managing Data Privacy and Cybersecurity Issues*, "Global Arbitration Review", 2021, p. 2, the document is available online at <https://globalarbitrationreview.com/guide/the-guide-evidence-in-international-arbitration/1st-edition/article/managing-data-privacy-and-cybersecurity-issues>.

³² Guillermo García-Perrote, *Admissibility of 'Hacked Evidence' in International Arbitration*, "Kluwer Arbitration Blog", 2021, the document is available online at <https://arbitrationblog.kluwerarbitration.com/2021/07/07/admissibility-of-hacked-evidence-in-international-arbitration/> (last accessed 30 March 2023).

- Arbitration Blog”, 2019.
3. Cristina Pop, EU vs US: What Are the Differences Between Their Data Privacy Laws?, 2022.
4. Emily Hay, *The Invisible Arm of GDPR in International Treaty Arbitration: Can't We Make It Go Away?*, “Kluwer Arbitration Blog”, 2019;
5. Erik G. W. Schäfer, Global Arbitration Review, Managing Data Privacy and Cybersecurity Issues, “Global Arbitration Review”, 2021.
6. Gerald Leong, *How Do You Deal With Data Protection And Cybersecurity Issues In a Procedural Order?*, “Kluwer Arbitration Blog”, 2020.
7. Guillermo García-Perrote, *Admissibility of 'Hacked Evidence' in International Arbitration*, “Kluwer Arbitration Blog”, 2021.
8. John Choong, Vasuda Sinha, Sofia Klot, Olivier André, *Data protection and cybersecurity in international arbitration remain in the spotlight*.
9. Martin Zahariev, *Data Protection in Commercial Arbitration: In the Light of GDPR*, Lambert Academic Publishing, 2019.
10. Martin Zahariev, *GDPR Issues in Commercial Arbitration and How to Mitigate Them*, “Kluwer Arbitration Blog”, 2019.
11. Pierre Bienvenu, Benjamin Grant, *Data protection and cyber risk issues in arbitration*, “*International arbitration report*”, issue 13, 2019.