DELab

DIGITAL RESEARCH STUDIES

WORKING PAPER # 2/2022

ARBITRATION AND THE PROTECTION OF PERSONAL DATA UNDER THE EU GENERAL DATA PROTECTION REGULATION

Autor: Karol Piwoński

Opieka naukowa: dr hab. Magdalena Słok-Wódkowska

CYTOWANIE

K. Piwoński, ARBITRATION AND THE PROTECTION OF PERSONAL DATA UNDER THE EU GENERAL DATA PROTECTION REGULATION, DELab Digital Working Studies 2/2022, Warszawa 2022

ABSTRACT

The far-reaching reform of the EU data protection regime has impacted many areas of social life, including the field of private dispute resolution (arbitration). The measures introduced and obligations imposed by the General Data Protection Regulation (GDPR) may turn out impractical in the context of arbitration and difficult to reconcile with its unique features, such as confidentiality, flexibility or efficiency. The paper outlines and attempts to address the most significant legal issues that arise at the intersection of arbitration and data protection laws. In the initial part, it discusses the application of the GDPR to arbitration proceedings and the lawfulness of the processing of personal data in the course of such proceedings. Next, the author addresses the problem of assigning appropriate roles under the GDPR to the participants of arbitral proceedings – such as the controller, processor, or data subject – while discussing the rights and obligations associated with them. The last chapter, devoted to the principles of personal data processing, indicates the obligations they impose in the context of arbitration, and the practical problems that may arise in the course of their implementation.

STRESZCZENIE

Dalekosiężna reforma unijnego systemu ochrony danych osobowych wywarła wpływ na wiele obszarów życia społecznego, nie omijając sfery prywatnego rozstrzygania sporów (arbitrażu). Rozwiązania wprowadzone przez ogólne rozporządzenie o ochronie danych (RODO) i obowiązki przez nie nałożone mogą okazać się niepraktyczne w kontekście arbitrażu i trudne do pogodzenia z jego unikatowymi cechami, takimi jak poufność, elastyczność czy efektywność. Praca zarysowuje i próbuje rozwiązać najistotniejsze problemy prawne występujące na styku arbitrażu i prawa ochrony danych osobowych. W początkowej części, omówiona została kwestia zastosowania RODO do postępowań arbitrażowych oraz dopuszczalności przetwarzania danych osobowych w toku tych postępowań. Następnie podjęto problem przypisania uczestnikom arbitrażu odpowiednich ról na gruncie Rozporządzenia – takich jak administrator danych, podmiot przetwarzający czy osoba, której dane dotyczą – omawiając jednocześnie prawa i obowiązki z nimi związane. Ostatni rozdział pracy, poświęcony zasadom przetwarzania danych osobowych, wskazuje na obowiązki płynące z nich w kontekście postępowań arbitrażowych i praktyczne problemy, jakie mogą wystąpić w toku ich implementacji.

I. INTRODUCTION

a) Foreword

May 2022 marked the beginning of the fifth year of the application of the General Data Protection Regulation[1]. This fundamental, standard-setting law has attracted significant attention as it introduced a new and radical approach to the protection of personal data, the omnipresence of which is the cornerstone of today's information society. The wind of change initiated by the Regulation has not spared the field of private dispute resolution, raising compliance-related concerns within the arbitration community[2].

So far, there has been little dialogue between data protection and arbitration practitioners. Both fields, however, are destined to coexist, interact, and possibly clash in the years to come. While globalisation has significantly increased the importance of international arbitration as a means of dispute resolution, digitalization has enabled a large amount of data to be circulated freely over vast distances, forcing its circulation in any arbitral proceedings[3].

Parties' pleadings, the evidence submitted, witness statements, expert reports, awards – all of these contain large amounts of personal data: names, surnames, dates of birth, home and email addresses, photos, audio recordings, bank account numbers and employment history, to name just a few. This data is shared with (and processed by) the parties, the arbitrators, the tribunals' secretaries, the arbitral institutions, the witnesses, the expert witnesses, in some cases with national courts or even with the public. A significant gap in the system for the protection of privacy

[1] The Regulation 2016/679 of the European Parliament and of the Council 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), hereinafter: GDPR or Regulation, came into force on May 25, 2018. When a reference is made to a legal provision of an unspecified legislative act, it refers to the GDPR.

[2] In the *2021 International Arbitration Survey*, „an overwhelming number of interviewees, across all regions and roles, expressly referred to this EU legislation when discussing data protection. Interviewees explained that they felt the GDPR in particular had brought the issue of data protection to the fore. As one observer stated, the GDPR put the issue of accountability in data processing operations in the context of arbitration on the table. The large fines potentially payable for non-compliance was thought to be a major factor in drawing attention to data protection issues". *See* the *2021 International Arbitration Survey: Adapting arbitration to a changing world*, https://www.whitecase.com/sites/default/files/2021-06/qmul-international-arbitration-survey-2021-web-single-final-v2.pdf, accessed: 6.04.2022, p. 30-31.

[3] K. Paisley, *It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration*, Fordham International Law Journal 2018, vol. 41(4), p. 845-846.

would exist if the processing of such data in the course of arbitral proceedings was not regulated by the law.

There is very limited authoritative, comprehensive guidance on how the GDPR text should be understood; its interpretation was described as „a journey into uncharted territory"[4]. This is equally applicable in the context of arbitration. While the GDPR introduces various principles of the processing of personal data, imposes numerous obligations on many actors and confers a number of rights on the data protection subjects, it does not specifically refer to arbitration, nor does it provide any instruction on how these principles, obligations and rights convert to the setting of arbitral proceedings.

The *2021 International Arbitration Survey* found that while arbitration practitioners generally acknowledge that data protection issues and regulations may have an impact on the conduct of arbitrations, „the extent and full implications of that impact are not understood by all"[5]. This paper seeks to contribute to increasing this understanding and to facilitate the meeting of the two worlds: arbitration and data protection.

b) The paper's structure

In the first chapter, a general introduction to the topic is offered. Moreover, the paper's structure, purpose and research methods are described. The author also explains the necessary reservations and limitations of the paper.

In the second chapter, three concepts of fundamental importance for the paper – its content and scope – are discussed. These include personal data, processing and arbitration. The author then provides an exemplification of the paper's premise that personal data is routinely processed in the course of arbitration proceedings.

The third chapter touches upon a question of particular significance: whether – and under what circumstances – does the GDPR apply to arbitration. The Regulation's material and territorial

[4] Ch. Kuner, L.A. Bygrave, Ch. Docksey and L. Drechsler, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press 2020, p. 2.

[5] The *2021 International Arbitration Survey*, *op. cit.,* p. 2.

scope are discussed – generally and with respect to arbitral proceedings seated in and outside of the EU. Moreover, the question of whether arbitration can be exempt from GDPR obligations is addressed.

In the fourth chapter, the issue of an appropriate legal basis for the processing of personal data in arbitration is discussed. The author describes various legal bases set out in the GDPR and argues which of them (and under what circumstances) can find application in the arbitration context. What is also mentioned is the lawfulness of the processing of sensitive data („special categories of personal data") in arbitration, which requires a separate legal basis.

The fifth chapter portrays the actors of arbitration and the actors of the GDPR in an attempt to „assign" appropriate data protection functions and obligations to participants of the arbitral proceedings. It is addressed if and when entities such as arbitral institutions, arbitrators, parties and parties' counsels can act as controllers or processors of personal data. Then, the author identifies the data subjects in the context of arbitration and provides an overview of their rights.

In the sixth chapter, principles of the processing of personal data are addressed. The content, scope and significance of the principles set forth in the Regulation, such as the lawfulness, fairness and transparency of data processing, purpose limitation or accuracy are analysed. Following a general introduction to each principle, more arbitration-specific reasoning is applied to assess what is the role of each of them in arbitral proceedings and how they affect their course, the functioning of arbitral institutions, as well as the rights and duties of the proceedings' participants. Moreover, the author discusses the timely issue of data transfer, which is of particular importance to arbitral proceedings of an international character.

The seventh chapter concludes the paper. The author indicates why strict compliance with the GDPR is a necessity for arbitration practitioners and discusses the desired developments in data protection laws in the arbitration context.

c) The paper's purpose and research methods

The purpose of this paper is to discuss if and how personal data is protected under the GDPR in the course of arbitral proceedings. The paper starts from the assumption that no dispute submitted to arbitration could be resolved without the processing of a large amount of personal data by

various participants of the proceedings. It will seek to verify that: (i) the processing of personal data in arbitration is governed by the GDPR; (ii) some processing activities are within the territorial scope of the Regulation's application; (iii) there is at least one legal basis that justifies the processing of personal data in the course of arbitral proceedings; (iv) each participant of the proceedings is responsible for GDPR compliance with respect to their own processing activities. The author will also discuss how the principles of the processing of personal data „translate" to the setting of arbitral proceedings and what is required of arbitral institutions, arbitral tribunals and other participants of the proceedings for their implementation.

Given limited guidance on arbitration-specific problems of protection of personal data, this paper aims to fill in the gaps and propose solutions that are legally sound, while at the same time practical and tailored to the specific features of arbitration. Thus, the author will try to reconcile the need for the strict observance of the GDPR with the reality of arbitral proceedings and their desired characteristics, such as efficiency, flexibility or confidentiality, hoping to contribute to reducing the risk that „GDPR compliance in each case will quickly paralyse or even overwhelm" the primary mission of arbitrators[6].

This paper is not intended to provide an exhaustive discussion of all aspects of data protection that arise in connection with arbitration proceedings, as such a comprehensive overview would exceed the permissible scope of the paper. Thus, a selection of relevant, most pressing problems had to be made. This selection is not completely subjective. To decide upon the matters to address, the author took into account, among others, existing scholarship, recent jurisprudence, and legislative developments.

The purpose of the paper will be accomplished by employing primarily the legal-dogmatic research method. The author will address the selected legal issues, analysing the text of the GDPR, the scholarship and the jurisprudence, as well as guidance from bodies such as the European Data Protection Board and posts published on professional blogs. Where appropriate, the author will present his own motivated views. To a lesser extent, the comparative method will be employed, in particular to compare the GDPR with former regulations and national data protection laws, to search for similarities and differences.

[6] A. Blumrosen, *The Allocation of GDPR Compliance in Arbitration* [in:] *International Arbitration EU Law,* J.R. Mata Dona and N. Lavranos (eds), Edward Elgar 2021, p. 95.

II. BASIC CONCEPTS: PERSONAL DATA – PROCESSING – ARBITRATION

This paper seeks to discuss how personal data is protected in arbitral proceedings. To do so, it is necessary to define these three fundamental categories: personal data, processing and arbitration.

a) Personal data

The crucial role of the term „personal data" stems from the fact that it is a threshold concept for the application of data protection law generally: if the data being processed are not personal data, the processing is not subject to such law[7]. While non-personal data do not fall within the scope of application of the GDPR, they do fall within the ambit of other EU legal instruments, such as Regulation 2018/1807 on a framework for the free flow of non-personal data in the European Union, which restricts Member States' ability to introduce or maintain data localisation requirements for non-personal data[8].

The term „personal data" was defined in Art. 4(1) of the GDPR and it means:

> „any information relating to an identified or identifiable natural person («data subject»)".

Importantly, the definition of „personal data" found in the GDPR is very similar to the one introduced by the DPD. Thus, the CJEU's jurisprudence on this matter before the GDPR is deemed to have retained relevance[9].

The definition of „personal data" relies on four elements: (1) „any information"; (2) „relating to"; (3) „identified or identifiable"; (4) „natural person".

[7] Ch. Kuner et al., *The EU General Data…, op. cit.*, p. 106.

[8] Ibid., p. 107.

[9] Ibid.

The first constituent element („**any information**") was interpreted by the CJEU in *Nowak*, where the Court found that the use of the expression „any information" in the definition of the concept of „personal data" reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it relates to the data subject[10].

Some real-world examples of personal data were provided by the European Commission and include the following:

- name;
- surname;
- home address;
- email address (such as name.surname@company.com);
- identification card number;
- location data;
- IP address;
- cookie ID;
- the advertising identifier of your phone;
- data held by hospitals or doctors, which could be a symbol that uniquely identifies a person[11].
- Data such as email addresses not containing names and surnames (such as info@company.com), anonymized data or a company registration number will not constitute personal data[12].

Enlightening remarks on this matter were also delivered by Advocate General Sharpston, pursuant to whom „the actual content of that information appears to be of no consequence as long as it relates to an identified or identifiable natural person. It can be understood to relate to any facts regarding that person's private life and possibly, where relevant, his professional life (which might

[10] Judgment of the Court of Justice of 20.12.2017, *Peter Nowak v Data Protection Commissioner*, ECLI:EU:C:2017:994, para. 34.

[11] European Commission, *What is Personal Data?,* https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en, accessed: 13.03.2022.

[12] Ibid.

involve a more public aspect of that private life). It may be available in written form or be contained in, for example, a sound or image"[13].

The CJEU in its jurisprudence has found numerous types of information to constitute personal data. These included, among others, a person's telephone number, information regarding their working conditions and hobbies, data on personal income and tax, passport details, fingerprints, images of persons recorded on a video camera, exam scripts and the comments of examiners on those scripts, as well as electronic communications traffic data, including, under certain circumstances, IP addresses[14].

The CJEU has also taken a broad view with respect to the second element of the definition of „personal data" („**relating to**)"[15]. In the *Nowak* judgment, the Court has found that this element is satisfied „where the information, by reason of its content, purpose or effect, is linked to a particular person"[16]. Generally speaking, information can be considered to „relate" to an individual when it is *about* that individual[17]. However, even when information primarily concerns an object – such as a smartphone – it still may constitute personal data, as indirectly relating to a particular person[18].

As regards the „**identified or identifiable**" element, it is important to note that it is the only element of definition which is defined in the Regulation. Article 4(1) provides that:

> „an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

This element is deemed to be satisfied even if the controller cannot make a link to a particular person without help from other sources. That is in line with the flexible approach suggested by the

[13] Opinion of AG Sharpston of 12.12.2013, Joined Cases C-141/12 and C-372/12, *YS*, ECLI:EU:C:2013:838, para. 45.

[14] CJEU, *Protection of Personal Data (Fact sheet)*, July 2020, https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf, accessed: 15.03.2022.

[15] Ch. Kuner et al., *The EU General Data…, op. cit.*, p. 111.

[16] Judgment of the Court of Justice of 20.12.2017, *Peter Nowak v Data Protection Commissioner*, ECLI:EU:C:2017:994, para. 35.

[17] Article 29 Working Party, *Opinion 4/2007 on the concept of personal data*, WP 136, 20.06.2007, p. 9.

[18] B. Van Alsenoy, *Data Protection…, op. cit.*, p. 26.

wording of the GDPR and its recital 26, which refers to „singling out", „either by the controller or by another person to identify the natural person directly or indirectly". Therefore, even pseudonymisation does not preclude that a person is „identified or identifiable", if they can still be attributed to a natural person by the use of additional information[19]. Importantly, however, identifiability is limited by a requirement that only the means „reasonably likely to be used" should be considered[20]. In *Bryer*[21], the CJEU confirmed that „it is not required that all the information enabling the identification of the data subject must be in the hands of one person"[22].

Turning to the fourth element of the definition of personal data („**natural person**"), it is important to note what is not covered by the Regulation. That includes primarily any types of legal persons, including any corporations or partnerships. The deceased persons are also considered not to be covered by the term „natural person", and thus do not „benefit" from the GDPR's protection, as was made clear in recital 27. Despite that, some Member States have decided to extend the protection of personal data to some period after one's death (Denmark, Italy), and are entitled to do so, as follows from said recital[23].

As companies are the predominant parties to arbitral proceedings, it is important to look closer if the data relating to them in some circumstances may be protected under the GDPR. In *Schecke*[24], the Court of Justice found that indeed, sometimes this may be the case. As stated by the Court, „in so far as the official title of the legal person identifies one or more natural persons", the legal person may claim the protection of data linked to it, pursuant to Articles 7 and 8 of the Charter"[25].

Given how broad the term „personal data" is, it becomes apparent that no arbitral proceedings could be completed without the involvement of large amounts of such data. The submissions of the parties, the evidence, the witnesses' testimonies, the expert reports, *amicus curiae* submissions, awards, orders – all of these will inevitably contain personal data: names and surnames,

[19] GDPR, recital 26.

[20] Ibid.

[21] Judgment of the Court of Justice of 19.10.2016, C-582/14, *Breyer*, ECLI:EU:C:2016:779.

[22] *Breyer*, para. 43.

[23] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 113.

[24] Judgment of the Court of Justice of 9.11.2010, Joined cases C-92/09 and 93/09, *Schecke*, ECLI:EU:C:2010:662.

[25] *Schecke*, para. 53.

home and email addresses, letters, emails, photos, audio recordings, bank account numbers, employment histories, health information and others.

b) Processing

Now I will turn to the second fundamental concept of the GDPR – processing. This term was defined in Art. 4(2) of the GDPR. Pursuant to the Regulation, it means:

> „any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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".

The definition of processing aims at: (1) preventing the risk of circumvention; and (2) ensuring the applicability of the GDPR irrespective of the techniques used to process data[26]. Again, the definition provided in the GDPR closely resembles the one in the DPD. The only differences between them are in the non-exhaustive list of examples of „processing" that they provide: the GDPR adds „structuring" to the list and replaces the term „blocking" – which was considered ambiguous – with the term „restriction"[27].

As is the case with the definition of „personal data", „processing" is extremely broad – in fact, any operation performed upon personal data by automatic means is covered by the definition of processing[28]. As noted in the scholarship, it is difficult to conceive any operation performed on personal data which would fall outside the definition of „processing"[29]. It should therefore be not surprising that the CJEU has found the term „processing" to refer to a wide range of different activities. To name a few examples, the following were found to constitute processing under the DPD or the GDPR:

---

[26] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 118.

[27] Ibid., p. 119.

[28] B. Van Alsenoy, *Data Protection..., op. cit.*, p. 27.

[29] Ibid.

- the loading of personal data on an internet page[30];
- the communication of personal data in response to a request for access to documents[31];
- the communication of the name and address of an internet subscriber or user[32];
- the activities of a search engine consisting in exploring the internet automatically, constantly and systematically in search of the information which is published there and the disclosure of such information in the form of lists of search results[33];
- the taking and storing of a person's fingerprints[34];
- the retention of data for the purpose of possible access to them by the competent national authorities[35];
- the video recording of persons[36];
- the transfer of personal data from an EU Member State to a third country[37];
- the transcription and keeping of personal data in a register and its communication to third parties[38];
- the drawing up of a list of individuals[39];
- the act of publishing a video recording, which contains personal data, on a video website on which users can send, watch and share videos[40];

Some examples of processing according to the European Commission include:

- staff management and payroll administration;
- access to a contacts database containing personal data;
- sending promotional emails;

[30] Judgment of the Court of Justice of 6.11.2013, C-101/01, *Lindqvist*, ECLI:EU:C:2003:596, para. 25. *See also* Judgment of the Court of Justice of 13.05.2014, *Google Spain*, C-131/12, ECLI:EU:C:2014:317, para. 26.

[31] Judgment of the Court of Justice of 29.06.2010, C-28/08 P, *Commission v Bavarian Lager*, ECLI:EU:C:2010:378, para. 69.

[32] Judgment of the Court of Justice of 19.04.2012, C-461/10, *Bonnier Audio*, ECLI:EU:C:2012:219, para. 52.

[33] Judgment of the Court of Justice of 13.05.2014, *Google Spain*, C-131/12, ECLI:EU:C:2014:317, paras. 26-31.

[34] Judgment of the Court of Justice of 17.10.2013, C-291/12, *Schwarz*, ECLI:EU:C:2013:670, paras. 28-29.

[35] Judgment of the Court of Justice of 8.04.2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238, para. 29.

[36] Judgment of the Court of Justice of 14.02.2019, C-345/17, *Buivids*, ECLI:EU:C:2019:122, para. 35.

[37] Judgment of the Court of Justice of 6.10.2015, C-362/14, *Schrems*, ECLI:EU:C:2015:650, para. 45.

[38] Judgment of the Court of Justice of 9.03.2016, C-398/15, *Manni*, ECLI:EU:C:2017:197, para. 35.

[39] Judgment of the Court of Justice of 27.09.2016, C-73/16, *Puškár*, ECLI:EU:C:2017:725, para. 103.

[40] Judgment of the Court of Justice of 14.02.2019, C-345/17, *Buivids*, ECLI:EU:C:2019:122, para. 39.

- shredding documents containing personal data;
- posting a photo of a person on a website;
- storing IP addresses or MAC addresses;
- video recording (CCTV)[41].

c) Arbitration

Arbitration is not an easily definable concept. Gary Born believes that arbitration is „a process by which parties consensually submit a dispute to a non-governmental decision-maker, selected by or for the parties, to render a binding decision resolving a dispute in accordance with neutral, adjudicatory procedures affording each party an opportunity to present its case"[42].

A detailed analysis of the term „arbitration" (alongside the terms „commercial" and „international") was delivered by Ph. Fouchard, E. Gaillard and B. Goldman. The authors conclude that „arbitration" should be defined by reference to two constituent elements. First, the arbitrators' task is to resolve a dispute; second, the source of this judicial role is a contract: the power of the arbitrators to decide a dispute originates in the common intention of the parties[43].

Polish scholars seem to generally agree with this approach, although they typically add additional elements to it. The term „arbitration" was defined by T. Ereciński and K. Weitz as „a method of resolving civil cases in which the adjudicating authority is not a state court and derives its jurisdiction, which excludes the jurisdiction of state courts, from the agreement of the parties"[44]. The authors further elaborate that the constitutive features of arbitration tribunals are: their non-state (private) character, the will of the parties as the source of authority to resolve the case, and the recognition of this authority by the law, with the effect of equating the legal force of arbitration court judgments with state court judgments[45].

---

[41] European Commission, *What constitutes data processing?*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en, accessed: 17.02.2022.

[42] G. Born, *International Arbitration: Law and Practice*, Kluwer Law International 2012, p. 5-6.

[43] Ph. Fouchard, E. Gaillard, B. Goldman, *Fouchard, Gaillard, Goldman..., op. cit.*, p. 11.

[44] T. Ereciński, K. Weitz, *Sąd arbitrażowy*, Warsaw 2008, p. 17.

[45] Ibid.

A similar definition was adopted by A. Szumański, who defines arbitration as „a means of binding settlement by a private court (arbitral tribunal) of an existing or future legal dispute arising in connection with a particular legal relationship between the parties to the dispute, generally of a commercial nature, which derives its authority from the will of the parties to the said dispute, while excluding the cognition of the state court (ordinary courts)"[46]. As there generally is a consensus on what the term „arbitration" entails, there is no need to choose among the provided definitions. In case of doubt whether any proceedings constitute „arbitration" (as opposed to, for example, litigation in national courts or other means of dispute settlement), such instances will be addressed separately.

In general, there are three types of arbitration: commercial arbitration, investment arbitration and state-to-state arbitration[47]. Commercial arbitration is, broadly speaking, any international arbitration between companies where the dispute is economic in character[48]. In other words, it is arbitration arising from commercial dealings between private parties[49]. It can also be defined as a „system for final determination of commercial disputes in a judicial manner by a private arbitral tribunal appointed for that purpose"[50].

On the other hand, investment arbitration involves investment disputes between foreign investors and host states[51]. State-to-state arbitration, or „interstate" arbitration, typically involves disputes between two states or state-like entities and often raises issues of public international law[52].

At this point, it should be underlined that this paper concerns primarily commercial arbitration. Other types of arbitration will not be addressed separately as giving them due attention would exceed the permissible scope of this paper. In view of many concerns as to the applicability of the GDPR to investment arbitration, this issue should be dealt with individually in the scholarship[53].

---

[46] A. Szumański, *Arbitraż handlowy* [in:] *System Prawa Handlowego*, t. 8, Warsaw 2015, p. 8.

[47] Ibid.

[48] Ibid., p. 35.

[49] G. Born, *International Arbitration…, op. cit.*, p. 41.

[50] *See* https://www.vicbar.com.au/public/adr/commercial-arbitration, accessed: 19.03.2022.

[51] G. Born, International Arbitration…, op. cit., p. 37.

[52] Ibid,

[53] *See* J. Huang, D. Xie, *Data Protection Law in Investment Arbitration: Applicable or Not?*, Arbitration International 2021, vol. 37(1), p. 167-196.

This does not mean, however, that the discussion in this paper is applicable to commercial arbitration only. Many addressed issues, regarding for example the principles of data processing, may equally concern arbitrations of all kinds.

d) Conclusion. Processing of personal data in arbitration

The term „processing" covers a wide range of activities typical for any arbitral proceedings. To conclude this chapter, it would be beneficial to provide an overview of the kind of activities typically undertaken in the course of arbitral proceedings which would qualify as the processing of personal data. These activities include in particular:

- document review, document retention, where the said document contains personal data; these actions would be considered processing specifically under the terms „collection" and „recording";
- staff management and payroll administration;
- access to database containing personal data;
- sending promotional emails, commonly undertaken by arbitral institutions.

All of these activities may involve „collection", „organization" and „storage" of personal data, thus amount to processing[54].

As suggested by A. Blumrosen, virtually any activity undertaken during an arbitration relating to documents including personal data is likely to be considered processing covered by the GDPR, even if it is just shredding documents or taking notes including the names of individuals[55]. Other authors list the following as examples of the processing of personal data: the collection and examination of documents, the transfer of documents to a counsel or an expert, the exchange of documents between the parties, or the disclosure of evidence ordered by the tribunal[56].

Interestingly from the perspective of arbitration, AG Sharpston held that legal analysis – understood as „a process controlled entirely by individual human intervention through which personal

[54] G.N. Ramani, *One size..., op. cit.*, p. 617.

[55] K. Paisley, *It's All About the Data..., op. cit.*, p. 864.

[56] A. Blumrosen, *The Allocation..., op. cit.*, p. 97.

data are assessed, classified in legal terms and subjected to the application of the law" – did not qualify as a form of „processing" for the purposes of Article 2(b) DPD[57]. The Court, however, did not explicitly approve nor disprove this view, finding that the process of legal analysis did not qualify as „personal data".

[57] Opinion of AG Sharpston of 12.12.2013, Joined Cases C-141/12 and C-372/12, *YS*, ECLI:EU:C:2013:838, paras. 62-65.

III. APPLICABILITY OF THE GDPR TO ARBITRATION

Having established that no arbitral proceedings could be completed without the processing of personal data, I will now look at whether this processing is governed by the GDPR, which would mandate compliance with various obligations imposed by the Regulation. This chapter, therefore, deals with a question essential to any discussion on the implications of data protection laws and arbitration, i.e., the applicability of the GDPR to arbitration proceedings. In line with the Regulation's structure, I will look separately at two dimensions of the GDPR's scope of application: its material and territorial scope.

Importantly, one must also note that even where the GDPR does not apply as a matter of law, some of its provisions may still apply as a matter of agreement. An example could include a transfer of personal data outside the EU, to entities or individuals who are not already subject to the GDPR. In such cases, transferors are required to make efforts to ensure that the personal data is protected after the transfer[58].

a) GDPR's material scope

i. Processing by automated means and manual processing in arbitration

Processing under the GDPR may generally take the form of processing by automated means (wholly or partially) or processing by other means. Processing by automated means (often called „automated processing") refers to all processing done by means of computer technologies, whereas processing other than by automated means primarily refers to any data processing operation executed by humans without the use of computing devices (often termed „manual processing")[59]. In most cases, processing by automated means will employ computer systems[60]. The

[58] International Council for Commercial Arbitration (ICCA), International Bar Association (IBA), *The ICCA-IBA Roadmap to Data Protection in International Arbitration (Public Consultation Draft),* February 2020, p. 7.

[59] Ch. Kuner et al., *The EU General Data…, op. cit.*, p. 120.

[60] P. Barta, M. Kawecki, P. Litwiński, *Art. 4* [in:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, P. Litwiński (ed.), Warsaw 2021, para. 5.

Regulation applies to any processing of personal data by automated means, whether wholly or partly[61].

The automated processing is omnipresent in the course of modern arbitral proceedings. The *ICC Commission Report on Information Technology in International Arbitration* provides many examples of devices which are employed in automated processing activities:

> „(i) email and other electronic communications between and among the parties, the arbitrator or arbitrators (the tribunal), and the administering body; (ii) storage of information for access by the parties and the tribunal using portable or fixed storage media (e.g. flash drives, DVDs, hard drives, and cloud-based storage); (iii) software and media used to present the parties' respective cases in an electronic format, rather than a paper format; and (iv) hearing room technologies (e.g. videoconferencing, multimedia presentations, translations, and „real time" electronic transcripts)"[62].

The use of all of these technologies typically involves the personal data, the storage and maintenance of which would amount to processing governed by the GDPR[63]. The same technologies are utilised on a daily basis by the arbitral institutions, the arbitrators, the parties' counsels, and other participants, making the processing subject to the Regulation.

While the substantial part of processing activities in the course of arbitral proceedings would involve automated means, the manual processing is also not irrelevant from that perspective. However, for manual processing to be governed by the GDPR, two conditions must be satisfied:

1) the personal data must be contained – or be intended to be contained – in a „filing system" (Article 2(1) GDPR); and
2) the „filing system" must be structured according to specific criteria (Article 4(6) GDPR)[64].

---

[61] Art. 2(1).

[62] *The ICC Commission Report on Information Technology in International Arbitration*, https://iccwbo.org/content/uploads/sites/3/2017/03/icc-information-technology-in-international-arbitration-icc-arbitration-adr-commission.pdf, accessed: 26.04.2022.

[63] G.N. Ramani, *One size..., op. cit.*, p. 619.

[64] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 120.

Pursuant to the definition of a filing system, which is found in Art. 4(6) of the Regulation, it means:

> „any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis".

It is a difficult task to assess whether personal data is processed manually if they do not form a part of a filing system. In the literature, it was suggested that this requirement should not be interpreted in the abstract, but on a case-by-case basis, looking at the circumstances of the particular processing[65].

To give an example, when a ticket inspector looks at an identity card in connection with an inspection in public transport, the GDPR will not apply as there is no filing system, nor intention to form a part of a filing system. However, if the inspector has made a note containing such personal data, the GDPR would start to apply[66].

Accordingly, if a letter or a photo containing personal data is shown to a witness during a hearing, this processing would not fall under the GDPR (with the witness as a controller). However, if documentation was sent to an expert witness to provide an opinion, the expert witness would then act as a controller with respect to personal data contained in the documents and this processing would be governed by the Regulation. This basis would also find application if an arbitral institution, arbitral tribunal or other entity keeps arbitration-related files in paper rather than in electronic form.

ii. Arbitration – an activity outside the scope of EU law?

To establish whether the GDPR applies to arbitral proceedings, I must also analyse the exclusions from the material scope of the Regulation, which are listed in Art. 2(2). These exclusions include the processing of personal data:

a) in the course of an activity which falls outside the scope of Union law;

---

[65] P. Barta, M. Kawecki, P. Litwiński, *Art. 4* [in:] *Ogólne rozporządzenie..., op. cit.*, para. 7.

[66] Ibid, para. 9.

b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU (which refers to common foreign and security policy);
c) by a natural person in the course of a purely personal or household activity;
d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safe-guarding against and the prevention of threats to public security.

At the outset, it becomes apparent that only the first exclusion merits further analysis. Obviously, commercial arbitration proceedings are not carried out by the Member States in connection with the common foreign and security policy (Art. 2(2)(b)). Moreover, they are not connected to purely personal or household activities of a natural person (Art. 2(2)(c)). This exclusion refers to an activity „with no connection to a professional or commercial activity"[67], which is clearly not the case with arbitration. They are also not connected to the prevention, investigation, etc. of criminal offences by competent authorities (Art. 2(2)(d)). Thus, the only moot point that may arise is whether arbitral proceedings constitute an activity falling outside the scope of EU law. This ground will now be further considered.

The Regulation's recitals give only one example of activities falling outside the scope of EU law, namely activities concerning national security[68]. An opinion was expressed in the scholarship that Art. 2(2) of the GDPR is to be read with the rules on the competences of the EU, enshrined in Art. 5 TEU and Art. 2-6 TFEU, pursuant to which the EU's competences may be exclusive, shared or supporting[69]. Arbitration as such – or any sphere of life that would cover arbitration – is not assigned to any of these categories. Thus, a strict and formalist interpretation could lead to the conclusion that arbitration is not within the EU's competences. Consequently, it would qualify as an activity which falls outside the scope of Union law and hence is not regulated by the GDPR.

[67] GDPR, recital 18.

[68] GDPR, recital 16.

[69] P. Barta, M. Kawecki, P. Litwiński, *Art. 4* [in:] *Ogólne rozporządzenie..., op. cit.,* para. 12.

That interpretation, however, may prove to be incorrect in light of the CJEU's jurisprudence. This exception – Art. 2(2)(a) – has been interpreted by the Court in *VQ v Land Hessen*[70]. The CJEU has referred to Art. 3(2) of the DPD, which excluded from the scope of the Directive:

- the processing in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union;
- processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters); and
- the activities of the State in areas of criminal law.

On this basis, the CJEU has referred to the activities mentioned by way of example in Art. 3(2) of the DPD – activities provided for by Titles V and VI of the Treaty on European Union and data processing operations concerning public security, defence, State security and activities in areas of criminal law – and argued that „those activities are intended to define the extent of the exception provided for therein, with the result that exception applies only to the activities which are expressly listed there or which can be classified in the same category"[71].

This interpretation seems somewhat *contra legem*, given that the Court has equated an example to an exception (introduced by the words „such as") with the limits of the exception. Consequently, the Court has left to interpretation a highly vague and presumably narrow term „activities which can be classified in the same category". This approach may run counter to a basic premise of the EU's competences, which is that they are limited to those conferred upon the EU by the Member States in the Treaties (principle of conferral)[72].

Admittedly, one would struggle to explain how arbitration is to be considered an activity governed by EU law. Perhaps, one could refer to one of shared competences – an area of freedom, security and justice (Art. 4(2)(j)). As can be learned from Art. 81 TFEU, judicial cooperation in civil matters covers also „the development of alternative methods of dispute settlement". It would still, however, be quite a stretch to find that this legal basis confers upon the European Union the compe-

[70] Judgment of the Court of Justice of 9.07.2020, C-272/19, *VQ v Land Hessen*, ECLI:EU:C:2020:535.

[71] *VQ v Land Hessen*, para. 69.

[72] TEU, Art. 5.

tence over arbitration or that arbitration is an activity governed by EU law. Notwithstanding the foregoing, the CJEU's restrictive interpretation of Art. 2(2)(a) allows one to expect that arbitration would likely be found to fall under the scope of the GDPR, but ultimately this issue can only be determined by a judgment of the Court of Justice.

A view that arbitration is not an activity governed by EU law was presented by an arbitral tribunal in a recent investment arbitration case, *Tennant Energy v Canada.* The tribunal found that the GDPR did not apply as arbitration was an activity falling outside the scope of EU law[73]. While the dispute was between non-EU parties: a US company and the government of Canada, one of the arbitrators was of a UK nationality (and residence), an EU Member State at the time. To support this finding, the tribunal simply observed that neither the EU nor any of its Member States are parties to NAFTA[74]. Despite the oversimplified argumentation, the view that arbitration is not an activity covered by EU law may resonate with arbitration practitioners as an easy – but uncertain – way out of GDPR obligations. Moreover, this finding may apply equally to both commercial and investment arbitration. It will be interesting to see the approach of other arbitral tribunals, inevitably facing the question of the applicability of the GDPR to their activities. It cannot be ruled out that this issue will become yet another point of contention between EU law and international arbitration[75].

b) GDPR's territorial scope

I have established that the processing of personal data in the course of arbitral proceedings may fall under the material scope of the GDPR. That does not mean that each arbitration from all over the world will be subject to the Regulation's obligations. To assess the participants of which proceedings must abide by the GDPR, I should now analyse the Regulation's territorial scope. The relevant rules are set out in Art. 3 of the GDPR.

[73] Tennant Energy, LLC (USA) v Government of Canada, PCA Case No. 2018-54, Procedural Order no. 2, 29.07.2019.

[74] J. Huang, D. Xie, *Data Protection Law...*, p. 174.

[75] *See, e.g.,* M. Słok-Wódkowska, M. Wiącek, *Zgodność dwustronnych umów inwestycyjnych pomiędzy państwami członkowskimi z prawem Unii Europejskiej. Glosa do wyroku TS z dnia 6 marca 2018 r., C-284/16*, Europejski Przegląd Sądowy 2018, vol. 11; G.A. Bermann, *European Union Law and International Arbitration at a Crossroads*, Fordham International Law Journal 2018, vol. 42.

Article 3 may be broken down into three parts: the first (Art. 3(1)) ensures that the GDPR applies to the processing of personal data by a controller or a processor with an establishment in the Union; the second (Art. 3(2)) extends the GDPR's application to a controller or a processor that lacks an establishment in the Union, under certain defined circumstances; the third (Art. 3(3)) addresses specific situations where Member State law applies by virtue of public international law[76].

i. Under Art. 3(1)

Under Art. 3(1), the Regulation 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".

Determining the territorial scope of the GDPR pursuant to Article 3(1) implies prior identification of the following elements:

- entity which is acting as a „controller" or „processor" of the processing;
- location of its „establishment";
- „context of [the establishment's] activities".

The question of which entity may act as a „controller" or „processor" in the arbitration context will be dealt with in chapter 6. At this point, I should deal with two questions: when the location of this entity's establishment is in the EU and what is the significance of the „context of activities" requirement.

As concerns the location of the establishment, the determination whether an entity based in the EU is to be considered an establishment of the controller or processor for the purposes of Article 3(1) should be made on a case-by-case basis and based on an analysis *in concreto*[77]. It was proposed that in the assessment of whether one is dealing with „an establishment in the Union", guidance should be taken from recital 22:

---

[76] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 84.

[77] European Data Protection Board, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*, 12.11.2019, p. 7.

> „[e]stablishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect".

Turning to the problem of the „context of activities", one should note that this criterion does not require that the processing in question is carried out by the relevant EU establishment itself, as long as it is carried out „in the context of its activities", as follows from the *Google Spain*[78]. The EDPB proposed that „with a view to fulfilling the objective of ensuring effective and complete protection, the meaning of «in the context of the activities of an establishment» cannot be interpreted restrictively"[79]. On the other hand, „the existence of an establishment within the meaning of the GDPR should not be interpreted too broadly to conclude that the existence of any presence in the EU with even the remotest links to the data processing activities of a non-EU entity will be sufficient to bring this processing within the scope of EU data protection law"[80]. To establish whether the processing was carried out „in the context of" the non-EU establishment's activities, attention should be given to the relationship between the data controller and processor and its local establishment in the EU, as well as revenue-raising in the EU by the local establishment[81].

ii. Under Art. 3(2)

In addition, the GDPR applies even when the controller or processor is not established in the Union, as stems from Art. 3(2). However, this basis only applies when the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

Thus, this legal basis refers to situations where it is not a controller or processor (or their „establishment") that is located in the EU, but the data subject. The recitals to the Regulation clarify that:

---

[78] Judgment of the Court of Justice of 13.05.2014, *Google Spain*, C-131/12, ECLI:EU:C:2014:317.

[79] European Data Protection Board, *Guidelines 3/2018..., op. cit.*, p. 7.

[80] Ibid.

[81] Ibid., p. 8.

> „whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union"[82].

Typically, parties from the EU participate in the arbitral proceedings conducted under the auspices of many international arbitral institutions, such as the LCIA, the HKIAC or the CIETAC[83]. These institutions arguably offer their dispute resolution services to EU businesses, but probably not to EU nationals (data subjects). Hence, a question arises if the requirement of „offering of goods or services to data subjects in the Union" should be understood as including only offering that targets data subjects directly[84].

The language of the recitals would suggest that in fact this provision is intended to cover sales to consumers[85]. If, however, a more flexible approach was to be adopted – which would be in line with the existing jurisprudence – activities such as translating arbitral rules into EU languages, visiting potential EU parties, posting information about EU-specific capabilities, sponsoring EU conferences, actively having their names included for consideration as arbitrators by EU institutions, or other similar activities, could amount to „offering of services", extending the application of the GDPR to foreign arbitral institutions[86].

It would be difficult, however, to extend this reasoning to arbitrators and arbitral tribunals based outside of the EU, since they are constituted only after the commencement of the proceedings and consequently they do not offer any „goods or services" to individuals. Apart from that, this

[82] GDPR, recital 23.

[83] *See, e.g., The LCIA 2020 Annual Casework Report*, https://www.lcia.org/media/download.aspx?MediaId=855, accessed: 22.04.2022.

[84] K. Paisley, *It's All About the Data…, op. cit.*, p. 866.

[85] Ibid., note 96.

[86] Ibid., p. 867.

legal ground will probably find limited or no bearing on arbitral proceedings, leaving the majority of them to be assessed in the light of Art. 3(1).

iii. Conclusion

There are many misconceptions concerning the scope of the GDPR. First, it is a widespread belief that GDPR obligations arise only when the processing concerns personal data of EU citizens[87]. What is crucial for the GDPR to apply is the controller or processor, not the data subject. The GDPR will apply to particular processing in the arbitration context if the controller or processor (e.g., the arbitral tribunal, the arbitral institution, or the claimant/respondent company) has an establishment located in the European Union and the particular personal data is processed in this establishment's „context of activities". The establishment will be located in the EU if the processing activity takes place in the EU and involves stable arrangements (is not occasional or incidental). This will particularly be the case if the processing involves the branch, a subsidiary, or any other form, irrespective of its legal status.

Second, it is an oversimplification that „any arbitration seated in the EU would be territorially covered by the GDPR – „since the seat of arbitration is in Europe – the control and the processing of personal data takes place in Europe"[88]. It should be emphasized that it is a simplification that arbitration is covered by the GDPR – the conduct of its participants is[89]. Each processing activity must be assessed independently. If the arbitration is seated in Paris and is conducted under the auspices of the ICC International Court of Arbitration, the processing involving the arbitral institution as a controller or processor will be governed by the GDPR, regardless of the data subject's nationality. On the other hand, if a Chinese arbitrator, with an establishment outside the EU, processed personal data of EU nationals, this situation would normally not fall under the scope of the GDPR, provided that there was no other factor connecting the processing to the EU.

This has been clearly set out in the VIAC's Privacy Statement, which reads: „The scope and applicability of the GDPR are not determined by the seat of VIAC or the seat of the proceedings, but by

[87] A. Respondek, T. Lim, *The Impact Of The „General Data Protection Regulation (GDPR)" On International Arbitration Proceedings*, September 2020, http://www.hk-lawyer.org/content/impact-%E2%80%9Cgeneral-data-protection-regulation-gdpr%E2%80%9D-international-arbitration-proceedings, accessed 15.04.2022.

[88] G.N. Ramani, *One size…, op. cit.*, p. 626.

[89] ICCA, IBA, *The ICCA-IBA Roadmap…, op. cit.*, p. 2.

whether the person responsible (e.g., party, arbitrator, other neutral third party, party representatives, translators, experts, etc.) is subject to the scope of application of the GDPR. Hence everyone participating in proceedings is obliged to verify if the GDPR is applicable to its data-processing and is to be qualified as a controller according to the rules of the GDPR"[90].

Finally, the processing of personal data of natural persons located in the EU may be governed by the GDPR, when the controller is a foreign arbitral institution that offered its services to them.

c) Can arbitration be exempt from GDPR obligations?

If arbitration is materially covered by the GDPR, a question must be asked whether it could benefit from any of the exemptions provided for in the GDPR or allowed in the GDPR to be established by the Member States.

i. Judicial capacity exemption

The first exemption provided for in the GDPR refers to „courts and other judicial authorities". With respect to such bodies, the competence of supervisory authorities under the GDPR was severely restricted. As explained in recital 20 to the Regulation:

> „[t]he competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations".

That is further confirmed by Art. 55(3) of the GDPR, pursuant to which: „[s]upervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capac-

[90] VIAC, *Arbitration Privacy Policy,* https://www.viac.eu/en/privacy-statement, accessed: 11.04.2022.

ity". The GDPR suggests instead that the judicial authorities themselves regulate the data used in the judicial capacity[91]. One should note that the exemption of Member State courts from oversight by the supervisory authority does not mean that the GDPR does not apply to the courts, rather, it means that the rules are enforced by the judicial authorities themselves rather than the supervisory authorities[92]. Some scholars call it „the right to self-regulate", which could be granted to other dispute resolution bodies, such as arbitral tribunals[93].

However, even though the recitals acknowledge the „out-of-court procedure"[94], the text of the Regulation did not follow through and provide for any special treatment to arbitration. Moreover, arbitration is not considered to be covered by the reference to „judicial authorities"[95]. First, arbitral institutions are not state bodies and remain private. Second, the judicial capacity exemption entails that said judicial authorities are supervised within the court system, which cannot be extended to arbitration, as it is independent and does not fall under the administrative supervision of national courts[96].

There is an apparent discrepancy in the GDPR's approach to the courts and to arbitral tribunals. Still, however, the judicial capacity exemption is not a valid legal basis to exclude arbitration from the competence of the supervisory authorities.

ii. Exemption under Art. 23 GDPR

While the Regulation applies to arbitration, the Member States may carve out special exceptions to limit the scope of the GDPR[97]. Pursuant to Art. 23, the scope of the obligations and rights provided for in the Regulation may be restricted – either by EU law or by Member State law – when certain conditions are met. These conditions are the following:

---

[91] K. Paisley, *It's All About the Data…, op. cit.*, p. 856.

[92] Ibid., p. 857.

[93] G.N. Ramani, *One size…, op. cit.*, p. 625.

[94] GDPR, recital 52.

[95] K. Paisley, *It's All About the Data…, op. cit.*, p. 857.

[96] Ibid.

[97] G.N. Ramani, *One size…, op. cit.*, p. 623.

1) the limitation refers only to the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22;
2) such a restriction respects the essence of the fundamental rights and freedoms;
3) such a restriction is a necessary and proportionate measure in a democratic society to safeguard values listed in the Regulation. These values include, among others, national security, defence, the protection of judicial independence and judicial proceedings, the enforcement of civil law claims, the protection of the data subject or the rights and freedoms of others or other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security.

The application of Art. 23 does not mean that a given activity is excluded from the GDPR, but rather that certain rights of the data subject do not apply[98]. This provision has significant potential to reconcile the need for strict observance of the GDPR with the realities of arbitral proceedings and the respect for substantive roles of the arbitration participants. An interesting, pro-arbitration approach was presented by K. Paisley, who argues that „[i]nternational commercial arbitration has a decision-making function, which is of a judicial character. Reconciling [data subject] rights with international arbitration will be challenging, and argues in favor of exempting data subject rights that are inconsistent with the cross-border, consensual, decision-making function of international commercial arbitration, and taking into consideration the fact that it is often confidential"[99].

An example of the application of this exemption is provided by an Irish regulation, which covers proceedings „before a court, statutory tribunal, statutory body, or an administrative or out-of-court procedure", thus including arbitration[100]. The Irish exemption limits the following data subject rights: to transparent information (potentially including data privacy notices) (Art. 12, 13 and 14), access to data (Art. 15), rectification and erasure (Art. 16 and 17), to restrict further processing (Art. 18), data portability (Art. 20) and the rights to object and to automated decision making

[98] K. Paisley, *It's All About the Data…, op. cit.*, p. 858.

[99] Ibid., p. 859.

[100] Ibid., p. 858.

(Art. 21 and 22)[101]. The Irish exemption was met with a positive reception in the scholarship. As argued by K. Paisley, the rights limited by the mentioned national legislation „are particularly difficult to apply to arbitration and can be inconsistent with the arbitrator's decision-making function, including the interactions among arbitrators, and with the institution"[102].

While the realistic outlook on the arbitral proceedings allows this view to be shared, this approach may be detrimental to the purpose of the GDPR, which was to bring uniformity in the application of data protection law[103]. It could lead to a situation where within one arbitration, the rights of the data subjects (and corresponding obligations of data controllers and processors) could be different depending on their nationality, which may undermine the equality of the parties to the proceedings[104].

Hence, depending on the future development of national laws and jurisprudence, an amendment to the GDPR – or at least arbitration-specific guidance from the EDPB – may turn out to be necessary, to adopt a universal approach toward the protection of data rights in the arbitration context, without posing a risk to the efficiency of the arbitral proceedings and to the uniformity of the application of the GDPR.

To conclude, on the basis of Art. 23, several rights of the data subjects could be limited, also as regards the processing of personal data in arbitration. However, this does not affect the general applicability of the Regulation to the arbitral proceedings. The significance of this provision is that the participants of the proceedings should be mindful of the national limitations applicable to them in the exercise of their data protection rights stemming from the Regulation.

[101] Ibid.

[102] Ibid.

[103] G.N. Ramani, *One size…, op. cit.*, p. 624.

[104] *See, e.g.,* I. Bantekas, *Equal Treatment of Parties in International Commercial Arbitration*, International & Comparative Law Quaterly 2020, vol. 69(4).

IV. Legal basis for the processing of personal data in arbitration

a. Introduction

I have already established that in every arbitral proceeding at least some – usually, large – amount of personal data is processed by various actors, and that this type of activity often falls under the scope of GDPR, mandating compliance of the involved arbitration actors. This chapter deals with the question of whether the processing of personal data in arbitral proceedings is lawful and if so, under which legal basis. It will also look at the consequences of relying on a particular legal base to justify processing.

Processing of personal data is only lawful under the GDPR if there is a legal basis applicable to the processing, as follows from Art. 6(1) of the Regulation. This provision stipulates that the processing of personal data is lawful only if and to the extent that at least one legal basis listed therein applies to the particular processing. Thus, the discussion of this chapter is closely connected to the principle of the lawfulness of the processing, which will be further elaborated in chapter 7.

What must be underlined at the outset is that there is no single legal basis that would allow for the processing of any personal data, by any entity and in any arbitration. Many different legal bases may be applicable to different cases of processing, depending on the circumstances, reasons for the processing and actors involved. This chapter will try to discuss if and when any of the six legal grounds set forth in Art. 6 of the GDPR may be lawfully invoked in the arbitration context.

There are six legal grounds for the processing of personal data. The catalogue is based on Article 7 DPD as it was believed that long experience in applying the DPD's provisions to the daily practice of information processing has confirmed that the list is comprehensive and serves well, even under rapidly changing technological-organisational developments[105]. Importantly, the catalogue of legal basis is exhaustive and the Member States are not allowed to add new principles relating to the lawfulness of the processing of personal data or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in that article[106].

[105] Ch. Kuner et al., *The EU General Data…, op. cit.*, p. 328.

[106] Judgment of the Court of Justice of 19.10.2016, C-582/14, *Breyer*, ECLI:EU:C:2016:779, para. 57.

b. Consent

The first legal basis for the processing of personal data is consent. This ground requires that the „the data subject has given consent to the processing of his or her personal data for one or more specific purposes" (Art. 6(1)(a)).

The cliché in arbitration reads that „consent is the cornerstone of arbitration"[107]. Consent, however, is not a likely cornerstone of the processing of personal data in arbitration. There are multiple reasons why this legal basis will not be appropriate for the processing of personal data in arbitration. These reasons include:

1) consent must be specific, informed and freely given;
2) consent must be obtained from the data subjects themselves rather than from the participant of arbitration who provides the personal data, including each data subject identified or identifiable from the submissions or evidence (not only the parties and the witnesses);
3) consent is likely to be an invalid ground in an employment context;
4) processing on the basis of consent may need to be stopped if consent is withdrawn or refused and it is difficult to then rely on another lawful basis for processing[108]; and
5) consent can be withdrawn freely at any time, which creates the risk of abuses.

Above all else, the reliance on consent in the arbitral setting is simply impractical. The consent would have to be obtained from each participant of the proceedings, by each controller, with respect to separate processing activities. To give an example, to process the personal data of the data subjects (witnesses, employees, business partners, etc.), contained in a party's pleading (the number of which may be several dozen), the consent of each of them would have to be obtained for the data to be lawfully processed by each controller: the arbitral tribunal, the arbitral institution and others.

[107] M. Zahariev, *GDPR Issues in Commercial Arbitration and How to Mitigate Them*, 7.09.2019, http://arbitrationblog.kluwerarbitration.com/2019/09/07/gdpr-issues-in-commercial-arbitration-and-how-to-mitigate-them/, accessed: 15.04.2022.

[108] ICCA, IBA, *The ICCA-IBA Roadmap..., op. cit.*, p. 17.

Moreover, one could wonder whether the consent given at the request of an arbitral tribunal fulfills the requirement of a consent „freely given". This condition has been elaborated on in recital 43, which may prove important from the arbitration perspective. The recital reads:

> „[i]n order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation".

While the arbitral tribunal is not a „public authority", it could still be argued that there is an imbalance as regards its relationship between, for example, an employee (data subject) and the employer or an arbitral tribunal. That is because to be able to provide or withhold consent for or against the processing of personal data, the data subject must have a real opportunity to provide/withhold consent without suffering any penalty. This real opportunity is unlikely to exist when the data subject serves under the capacity of the controller (e.g., employer company)[109].

This is not to say that consent as a legal basis in arbitration should be entirely disregarded. Rather, whenever possible, other bases should be relied on. It could still be useful to rely on consent in some circumstances, for example with respect to *amicus curiae* submissions or personal data of expert witnesses.

It is yet to be seen how specific the consent must be to constitute a valid legal ground for the processing of personal data in the dispute resolution setting. Under the GDPR, when the processing has multiple purposes, consent should be given for all of them[110]. Thus, it remains an open question whether one could consent to the processing of his or her personal data generally for the purpose of „dispute resolution proceedings" (for example in an employment contract), or if a valid consent has to be expressed separately for each individual case.

[109] G.N. Ramani, *One size…, op. cit.*, p. 620.

[110] GDPR, recital 32.

It is important to note that consent is the only legal basis so extensively regulated by the GDPR (it is governed also by Art. 7 and 8), thus participants of arbitral proceedings should be mindful of other requirements that must be satisfied for a consent to be valid.

c. Performance of a contract

The processing of personal data is lawful when it is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract (Art. 6(1)(b)).

This legal basis, such as several others, refers to „necessity". The concept of necessity, which has a long history in EU law, requires an assessment in light of the proportionality test: the authority adopting a measure which interferes with a right protected by EU law in order to achieve a legitimate aim must demonstrate that the measure is the least restrictive for the achievement of this aim[111]. These remarks find application to other legal bases prescribed in Art. 6(1) of the GDPR which refer to „necessity".

The legal basis found in Art. 6(1)(b) requires that the data subject was a party to a contract and that the processing of personal data of this subject was necessary for the performance of this contract. While it is not expressly stated in the provision, it is understood that this legal basis applies when processing data about one's contractual partner (the data subject) is necessary for the fulfilment of a contract by the other contractual partner (the controller)[112].

Admittedly, any arbitration takes its basis in the arbitration agreement between the parties. This contract, however, cannot constitute a basis for the processing of personal data by the arbitral institution or by the arbitrators, simply because they are not the parties to the arbitration agreement – the parties to the dispute are. As noted in the scholarship, „sub-clause (b) cannot be applied since the agreement to arbitrate in a commercial arbitration is between two commercial entities, whereas the clause requires the data subject to be party to the agreement"[113].

[111] Opinion of Advocate General Maduro of 3.04.2008, C-524/06, *Huber*, ECLI:EU:C:2008:194, para. 27.

[112] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 331.

[113] G.N. Ramani, *One size..., op. cit.*, p. 620.

Thus, this legal basis is unlikely to find broad application in the arbitration context, but is not entirely irrelevant. The „performance of a contract" ground could be invoked, for example, by an arbitral tribunal, when processing the personal data of an expert witness, who prepared an expert opinion on the basis of a contract he/she has concluded with the arbitral tribunal[114]. This also applies to an expert of a party, who prepared an opinion by order of that party.

d) Compliance with a legal obligation of the controller

Another legal basis allows for the processing of personal data when the processing is necessary for compliance with a legal obligation to which the controller is subject (Art. 6(1)(c)).

The „legal obligation" required under Art. 6(1)(c) of the GDPR must stem from a Union law or Member State law[115]. This provision should be understood as relating only to obligations that originate directly from a provision in the law and not from any contractual stipulation between private natural or legal persons[116]. Arbitration is governed by these laws only on an exceptional basis and does not normally impose any obligations concerning the processing of personal data in the course of arbitral proceedings.

What is crucial from the arbitration perspective is that the order of an arbitral tribunal, in all probability, will not be considered to constitute a „legal obligation", which would justify the processing of personal data. The WP29 opined that an obligation imposed by a foreign legal statute or regulation would not qualify as a „legal obligation" unless member state law requires compliance with an order of a foreign court[117]. As argued by G. Ramani, adopting the same standard in the context of an order of an arbitral tribunal calling for evidence, such an order would not be a legal obligation unless member state law mandates compliance with orders/rulings of a private arbitral tribunal[118]. Therefore, the parties and other entities required by the arbitral tribunal to present particular evi-

---

[114] M. Burianski, *Data Privacy in International Arbitration*, 19.10.2018, https://www.whitecase.com/publications/alert/data-privacy-international-arbitration, accessed: 21.04.2022.

[115] GDPR, recital 45.

[116] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 333.

[117] Working Party 29, *Working Document 1/2009 on pre-trial discovery for cross border civil litigation*, 11.02.2009, WP 158, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf, accessed: 21.04.2022, p. 9.

[118] G.N. Ramani, *One size..., op. cit.*, p. 622.

dence may invoke data protection laws as an impediment to the order, provided that there is no other basis that would justify the processing. Importantly, this obstacle can be removed, for example, by pseudonymisation of the relevant portions of personal data[119].

For these reasons, the ground for the processing of personal data enshrined in Art. 6(1)(c) will generally not find application in arbitration. However, an exception to this may include post-arbitration proceedings, for the purpose of which an arbitral institution may be required to submit to relevant courts the documents related to the arbitration. It may also include other instances where national courts interfere in arbitration proceedings.

e) Protection of vital interests of the data subject or another person

A legal basis enshrined in Art. 6(1)(d) stipulates that the processing of personal data is lawful when it is necessary in order to protect the vital interests of the data subject or of another natural person.

The recitals to the Regulation clarify the term „vital interests", stating that „the processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person"[120]. Further, it is stated that: „[s]ome types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters"[121]. In the literature, it was proposed that processing data on grounds of „vital interests requires that a situation of concrete and imminent danger exists for the data subject or a third (natural) person[122].

The narrow definition of „vital interests' under Art. 6(1)(d) makes the legal ground for data processing enshrined therein of little importance for arbitration. While some proceedings aim to safe-

[119] For the definition of pseudonymisation, see GDPR, Art. 4(5).

[120] GDPR, recital 46.

[121] Ibid.

[122] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 335.

guard vital economic interests of a given person or entity, such interests would not justify the processing of personal data under this legal basis[123].

f) Public interest or official authority of the controller

The penultimate legal basis for the processing of personal data, found in Art. 6(1)(e), states that processing is lawful when it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

This provision is the general basis for the lawful processing of personal data for public sector purposes[124]. The reason for processing under Article 6(1)(e) is the fact that it is necessary for a task, which „shall be carried out in the public interest or in the exercise of official authority" and has been „entrusted to the controller"; vesting such a task in a controller requires a legal provision to this effect[125].

This legal basis in all probability will find no use in arbitration. Data controllers in arbitration – e.g., arbitral institutions or arbitrators – do not carry out tasks in the public interest, but rather in the private interest of the parties to a particular dispute. Moreover, such controllers do not act in the capacity of a public authority as they remain private entities. As such private entities, operating on a commercial basis, they are not covered by this legal provision, even if they were vested with a task pursued in the public interest[126].

g) Legitimate interests pursued by the controller or a third party

The last legal basis, enshrined in Art. 6(1)(f), proclaims that the processing of personal data is lawful when it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. This ground, however, is not applicable „where such interests are overridden by the

[123] *See also* G.N. Ramani, *One size…, op. cit.*, p. 620.

[124] Ch. Kuner et al., *The EU General Data…, op. cit.*, p. 336.

[125] Ibid.

[126] Ibid., p. 337.

interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child"[127].

A „legitimate interest" is an interest which is visibly, although not necessarily explicitly, recognised by law, more precisely by Union or Member State law[128]. Such legitimate interest could exist, for example, where there is a relevant and appropriate relationship between the data subject and the controller, in situations such as where the data subject is a client or in the service of the controller[129]. Particular relevance must be attributed to the fundamental rights and freedoms recognised in the Charter as they are all potential sources of legitimate interests[130].

This legal basis is deemed to be generally „best suited" to data processing in the context of arbitration[131]. Moreover, the WP29 has opined – with respect to civil litigation in the United States – that the processing of personal data is justified on this basis in the context of discovery and collection of evidence to support or defend a legal claim[132]. This approach has also been adopted by the VIAC, which refers to the legitimate interests of the VIAC and the parties to the proceedings as the legal basis for the processing of personal data contained in „letters and documents, such as pleadings, witness statements, arbitral awards and other evidence or annexes"[133].

The importance of defending a legal claim does not take precedence over the fundamental rights of the data subjects who have no direct involvement with the claim[134]. In such situations, the controllers are obliged to perform a balancing act and weigh the necessity for processing evidence, i.e. processing personal data against the rights and freedoms of the data subject[135].

An interesting and controversial opinion was expressed in the scholarship that „unlike sovereign judges, private arbitrators do not hold the necessary authority or legitimacy to perform such bal-

[127] GDPR, Art. 6(1)(f).

[128] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 338.

[129] GDPR, recital 47.

[130] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 338.

[131] ICCA, IBA, *The ICCA-IBA Roadmap..., op. cit.*, p. 18.

[132] Working Party 29, *Working Document 1/2009 on pre-trial discovery for cross border civil litigation*, 11.02.2009, WP 158, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf, accessed: 19.04.2022.

[133] VIAC, *Arbitration Privacy Policy,* https://www.viac.eu/en/privacy-statement, accessed: 21.04.2022.

[134] Ibid.

[135] G.N. Ramani, *One size..., op. cit.*, p. 622.

ancing acts and determine questions involving fundamental rights of natural persons" and thus „Article 6(f) does not work as a concrete basis for lawful the processing of arbitral data"[136]. I am not convinced by this assessment. Arbitrators are not the only entities that may be obliged to perform such a „balancing act" – this legal basis may find a vast application in many spheres of life, where many entities will operate as „controllers", the majority of which will be much less qualified to perform such a test of competing interests. There are no strong arguments why any of such controllers – let alone, arbitrators – should be deprived of the right of conducting such assessments, and thus of relying on this legal basis.

It is the duty of the controller to assess whether the invocation of Art. 6(1)(f) was justified and this assessment remains under the control of the supervisory authorities. Guidance for this test has been offered by the WP29, which opined that:

> „[t]his balance of interest test should take into account issues of proportionality, the relevance of the personal data to the litigation and the consequences for the data subject. Adequate safeguards would also have to be put in place and in particular, there must be recognition for the rights of the data subject to object [to the processing] and, in the absence of national legislation providing otherwise, there are compelling legitimate grounds relating to the data subject's particular situation"[137].

I believe that while not being ideal, the legal basis referring to „legitimate interests" has the potential of covering the majority of the processing activities in arbitration context, although it is limited by the need for „legitimate interests" of the controller or third party on the one hand and by „fundamental rights and freedoms" of the data subjects on the other. For example, the data subject rights might override the legitimate interest if the processing could raise significant risks to a data subject's profession or personal life and the personal data is not likely to be case determinative[138].

In general, private dispute resolution, arbitration included, serves to strengthen one's access to justice and thus resolution of a dispute provides a valid, legitimate interest. Importantly, a controller may process data not only on behalf of their own legitimate interests but also because of the

[136] Ibid.

[137] Working Party 29, *Working Document 1/2009..., op. cit.*, p. 9-10.

[138] ICCA, IBA, *The ICCA-IBA Roadmap..., op. cit.*, p. 18.

legitimate interests of third parties. Thus, a valid justification for the processing of personal data in arbitration could be the interest of the parties to have their dispute resolved.

The assessment of whether the interests or fundamental rights and freedoms override the legitimate interests of the controller or a third party may be a difficult challenge for arbitration practitioners, but is necessary to ensure compliance with Art. 6(1) of the Regulation. A controller intending to rely on Article 6(1)(f) must therefore perform a special „balancing test", in accordance with the principle of proportionality[139]. The WP29 has offered a set of criteria for carrying out this test, which include the following:

- „assessing the controller's legitimate interest;
- impact on the data subjects;
- provisional balance; and
- additional safeguards applied by the controller to prevent any undue impact on the data subjects"[140].

Thus, the controller should take into account whether the processing of personal data is material to the outcome of the case and whether a particular fact can be established using other, less personal data-invasive means of inquiry. This assessment must be done before starting any processing operations based on Article 6(1)(f) and has to be properly documented in order to demonstrate that the controller's obligations have been fulfilled, as required under the principle of accountability[141].

It is important to note that in a situation of joint controllers, where the legal basis for the processing refers to „legitimate interests" of the processors, from the CJEU's jurisprudence it follows that it is necessary for each of those controllers to pursue such a legitimate interest[142]. This may be relevant for different participants of the arbitral proceedings – e.g., the arbitrators and the arbitration institution – acting as joint controllers.

[139] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 339.

[140] WP29 2014 p 33. See Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 339.

[141] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 339.

[142] Judgment of the Court of Justice of 29.07.2019, C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, para. 96.

One should also keep in mind that the processing for „legitimate interests" is anyway limited to what is plausibly necessary to pursue this interest; in line with the principle of proportionality processing can only be acknowledged as „necessary", if there is no better suited and less intrusive alternative available[143].

h) The processing of sensitive data

The processing of sensitive data – „special categories of personal data", as the GDPR puts it – is governed by a separate set of rules, enshrined in Art. 9 of the GDPR. At the outset it is important to note that under Art. 9 of the GDPR, any processing of sensitive data is prohibited, unless an appropriate legal basis for the processing can be justifiably applied. Due to their number and complexity, the limitations of the thesis make it impossible to discuss each of them separately with respect to arbitration. Thus, this section will only deal with the basic problems stemming from the processing of this category of personal data in arbitral proceedings.

As follows from Art. 9(1) of the GDPR, the special categories of personal data include personal data revealing:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs or
- trade union membership,

It also includes the processing of:

- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- data concerning health; or
- data concerning a natural person's sex life or sexual orientation.

In what circumstances are sensitive personal data processed in arbitral proceedings? One example could include arbitral proceedings arising out of mergers & acquisitions (M&A), which are globally

[143] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 339.

on the rise[144]. In such proceedings, typically a large amount of personal data gathered in the course of due diligence investigations is processed. The information sought in this process includes in particular „data associated with the acquired target (or acquired assets), such as data relating to employees, customers, users, contractors, suppliers and business partners"[145], which may obviously contain personal data revealing, e.g., employees' trade union membership, opinions and beliefs (political, religious, etc.), health, and other records having the character of sensitive data. Also, any documents relating to business valuation – also processed in the course of post-M&A disputes – would normally include some sensitive data, in particular concerning trade unions, health, and potential liabilities.

This problem may prove particularly significant also with respect to disputes involving the pharmaceutical, life sciences and healthcare sectors (for example disputes concerning the development of drugs or products disputes concerning regulatory approvals), where typically a large amount of sensitive, health-related data of the company's customers (e.g., medical records) is contained in the companies' information systems[146].

In virtually any proceedings, the submitted evidence may include some sensitive data, whether in the form of emails, notes, audio recordings, photos, reports, digital records, etc. The participants of the proceedings should be particularly cautious about such data and refuse to process it, unless it can be justified under the GDPR.

So, can sensitive data be legally processed in arbitration? Not surprisingly, that depends on the specific circumstances of the particular processing activity. In general, the processing of the special categories of personal data can be justified under the legal basis enshrined in Art. 9(2)(f) of the GDPR, which reads as follows: „Paragraph 1 [prohibition of the processing of sensitive data] shall not apply if one of the following applies: (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity". This exception is

---

[144] G. Vannieuwenhuyse, The Rise of M&A Arbitration, Kluwer Arbitration Blog, 6.04.2021, http://arbitrationblog.kluwerarbitration.com/2021/04/06/the-rise-of-ma-arbitration/, accessed: 21.04.2022.

[145] D. Ilan, *Privacy in M&A Transactions: Personal Data Transfer and Post Closing Liabilities*, 10.11.2016, https://corpgov.law.harvard.edu/2016/11/10/privacy-in-ma-transactions-personal-data-transfer-and-post-closing-liabilities/#:~:text=M%26A%20transactions%20often%20involve%20the,contractors%2C%20suppliers%20and%20business%20partners, accessed: 21.04.2022.

[146] *Why international arbitration is ideally suited for the Life Sciences and Healthcare sector*, 23.02.2021, https://www.osborneclarke.com/insights/international-arbitration-ideally-suited-life-sciences-health-sector, accessed: 25.04.2022.

called the „legal claims derogation". However, it will be applicable only in some situations, especially when the processing is likely to have a significant impact on the claimant or respondent's case[147]. Apart from that, sensitive data can also be processed when it has been „manifestly" made public by the data subject themselves (art. 9(2)(e)).

i. Conclusion

In this chapter, I have discussed the legal bases for the processing of personal data listed in Art. 6(1) of the GDPR. With respect to arbitration, it is important to note that there is no one universal legal basis for data processing. The decision as to which legal basis to rely on for processing purposes in a given arbitration proceedings is fact-driven and case-specific[148]. Moreover, the lawful bases may be different for different participants of the proceedings and for different processing activities[149].

The ground that will primarily find application in the arbitration setting refers to the legitimate interests pursued by the controller or a third party, while the remaining legal bases will be of use only in very specific circumstances. However, strict compliance with this legal basis – i.e. obligation to perform a special and documented test of weighing „legitimate interests" in processing against the legitimate interests of the data subject[150] – may be difficult to follow in the course of arbitration, given the number of data processing activities on the part of an arbitrator (or a group of arbitrators).

I also indicated the legal basis that is most likely to allow for the processing of sensitive data in arbitration – the „legal claims" ground, enshrined in Art. 9(2)(f) of the GDPR.

[147] ICCA, IBA, *The ICCA-IBA Roadmap..., op. cit.*, p. 18.

[148] Ibid., p. 16.

[149] ICCA, IBA, *The ICCA-IBA Roadmap..., op. cit.*, p. 16-17.

[150] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 339.

WHO IS WHO: GDPR ACTORS AND ARBITRATION ACTORS

a. Introduction

Every arbitration has its actors. These include, most importantly, parties to the dispute and the person or persons responsible for resolving it: the arbitrators. It is also typical for arbitral proceedings to include parties' counsels, witnesses, expert witnesses, arbitral institution, tribunal secretary (or secretaries), *amici curiae*, and others. The GDPR also has its own actors. The processing of personal data involves various entities: processors, controllers, data subjects, recipients, third parties and others. All of the participants of the arbitral proceedings may engage in the processing of personal data. They may also have their personal data processed by other participants.

The consequence is that arbitration participants take up different GDPR roles, as well as the rights and obligations associated with them. To describe how personal data is protected in the course of arbitral proceedings, it is thus necessary to consider *who is who* – which participants of arbitration typically act as controllers, processors, etc. In other words, this chapter deals with the allocation of data protection roles among the participants of arbitral proceedings.

b. Data controllers in arbitral proceedings

i. Who is a „data controller"?

There are two fundamental categories of entities that engage in the processing of personal data: controllers and processors. Under the GDPR, a „**controller**" is:

> „the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"[151].

[151] The Regulation clarifies in Art. 4(7) that „where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".

Controllers are key actors in the operationalisation of data protection law as they are the primary bearers of the obligations set by such law towards data subjects[152]. The concept of „controller" must be understood in light of the legislator's aim of placing primary responsibility for protecting personal data on the entity that actually exercises control over the data processing, which entails taking account not simply of legal formalities but factual realities[153].

According to the jurisprudence of the CJEU, the concept of controller is to be construed broadly so as to achieve effective and complete protection of the data subjects[154]. What is also relevant for the status of „controller" is the perspective of the data subject. According to the WP29, „the image given to data subjects and reasonable expectations of the data subjects on the basis of this visibility" are relevant factors[155].

The test of a controller may seem not complicated, referring to one ground only: the *determination of the purposes and means* of the processing of personal data. However, its practical application may cause numerous problems in practice.

The term „purposes" connotes the reason and objective for processing – in other words, the „why" of such processing. The term „means" is to be construed broadly as connoting the „how" of such processing, and this encompasses both technical and organisational elements, including the platform for data processing, the accessibility of the data, where the data is stored and for how long[156].

The element that is considered crucial is the determination of purposes – if a controller delegates this function to another entity it ceases to be a controller[157]. Some aspects of the means of processing may be delegated to others (namely, processors) without the controller thereby losing controller status[158].

---

[152] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 147.

[153] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 148.

[154] Judgment of the Court of Justice of 10.07.2018, C-25/17, *Jehovan todistajat*, ECLI:EU:C:2018:551, para. 21.

[155] Working Party 29, *Opinion 01/2010 on the Concepts of „Controller" and „Processor"*, 16.02.2010, WP 169, p. 12.

[156] Ibid., p. 14.

[157] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 150.

[158] Working Party 29, *Opinion 01/2010..., op. cit.*, p. 15.

Regarding the criterion „determine", this is to be understood as broadly denoting the ability to exercise influence. To attain controller status, it is sufficient that „a natural or legal person [...] exerts influence over the processing of personal data, for his own purposes, and [...] participates, as a result, in the determination of the purposes and means of that processing"[159]. It is not necessary for the status of a „controller" to establish that it had access to the data[160].

I should also mention that in the literature, it was confirmed that data subjects should not be considered „controllers" of their own personal data[161]. Undeniably, it would be nonsensical to require that a data subject comply with the obligations that are imposed on controllers under the GDPR, as such obligations are imposed on controllers specifically to protect others' interests (i.e. those of the data subjects), not their own[162].

ii. Data controllers' obligations

Some obligations of the data controllers (and processors) include the obligation to:

- adopt technical and organizational measures to ensure a level of security appropriate to the risk, including among other things, the anonymization and encryption of personal data[163];
- communicate to data subjects, at the time of data collection, : (i) the contact details of the controller(s) and processor(s); (ii) the purpose and the legal basis of the processing; (iii) the legitimate interests pursued by the controller by the processing; (iv) where applicable, the intention to transfer personal data to a country, third parties and the existence or absence of an adequacy finding; (v) the duration of data retention and/or the criteria used to determine the duration; (vi) the existence of the right to apply to the data controller to access personal data, the correction or deletion of such data, or a limitation of the processing operation relating to the data subject, or the right to object to the processing, and the right to

[159] *Jehovan todistajat*, para. 68.

[160] Ibid., para. 75.

[161] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 155.

[162] *Google Spain*, para. 34.

[163] GDPR, Art. 32.

data portability; (vii) the existence of the right to withdraw one's consent at any time; and (viii) the right to lodge a complaint to a supervisory authority[164].

As noted in the scholarship, „this requirement is perhaps the most confounding for arbitrators, as they are far removed from the original collection of the data, and have no connection with the data subjects who are typically – if I look beyond the arbitration participants – the employees, vendors or customers of the parties"[165]. Importantly, Art. 14 of the GDPR provides for less burdensome disclosure requirements for the processing of personal data that are not directly collected from the person concerned, and even these reduced obligations may be shifted by contract to the parties[166]. Still, as noted by K. Paisley, „if applied literally, this could mean potentially tens of data controllers being required to send multiple data privacy notices to potentially hundreds of individual data subjects named in the evidence. Serious concerns have also been raised about data subjects relying on these rights to request data relating to the confidential tribunal communications, potentially including draft awards"[167].

- rectify the inaccurate personal data upon the data subject's request[168].

In the scholarship, it was suggested that „there is no exception to this Article 16 data subject right that could apply to an arbitration proceeding, unless a Member State exempts such data under Article 23 of the Regulation, and so arbitration data protection protocols will need to identify a process in the arbitration to accommodate any requests based on this provision"[169]. However, this right should not be understood as allowing for the altering of evidence in arbitration[170].

[164] GDPR, Art. 13.

[165] A. Blumrosen, *The Allocation…, op. cit.*, p. 101.

[166] Ibid.

[167] K. Paisley, *It's All About the Data…, op. cit.*, p. 908

[168] GDPR, Art. 16.

[169] A. Blumrosen, *The Allocation…, op. cit.*, p. 101.

[170] Working Party 29, *Working Document 1/2009…, op. cit.*, p. 12.

The right to erasure, contained in Art. 17 of the GDPR, is less likely to influence arbitral proceedings, as it will not apply if the personal data is transferred „for the establishment, exercise or defence of legal claims"[171].

iii. Data controllers in arbitration

While, as I have established, it is not possible to predetermine „who is who" in arbitration from the GDPR perspective, it's undeniable that some participants of any arbitral process more likely than others to act in the capacity of „controllers" or „processors" rather than data subjects. This includes, in particular, the arbitral institution and the arbitrators. So, who normally possesses the status of a „controller" in the context of arbitral proceedings?

Not surprisingly, that must be assessed on a case-by-case basis, depending on the circumstances of the particular processing activity[172]. To elaborate, I need to discuss the ordinary „flow" of personal data in the arbitration setting. This is well illustrated by the following example:

> „To prepare a claim, a party collects documents containing personal data that it provides to its outside legal counsel. Counsel distils from those documents the relevant information, which includes personal data, and records that information in submissions and evidence, which is then provided to the administering institution and the tribunal. In order to perform their duties, the institution and arbitrators process the personal data contained therein[173]".

In this scenario, the party, its legal counsel, the institution and the arbitrators are all likely to be data controllers and thus subject to the rules established in the applicable data protection laws for data controllers. Their potentially overlapping individual compliance responsibilities create competing obligations that need to be reconciled[174].

---

[171] GDPR, Art. 17(3)(e).

[172] G.N. Ramani, *One size…*, *op. cit.*, p. 625.

[173] ICCA, IBA, *The ICCA-IBA Roadmap…*, *op. cit.*, p. 9-10.

[174] Ibid.

In the situation given, arbitral participants considered to be „controllers" will only be responsible for their own processing of personal data, not that of the others. Thus, it is impossible to predetermine which one natural or legal person will have the status of the „controller" in any arbitration. All participants of the proceedings may simultaneously be „controllers" with respect to some processing activities, and „data subjects" with respect to others. Thus, one can only establish the criteria relevant to this determination.

Dealing with **arbitral institutions** first, I should start by defining their role as, generally, administering arbitrations according to the institution's rules and practices[175]. As this often requires the parties to include the institution in communications exchanged with the tribunal, including all filings, the arbitral institutions have a central role in assisting the parties, and the arbitrators, organise the communication of information that may include personal data[176].

There are very strong arguments for allowing for such institutions (or in case they do not have separate legal capacity – the commercial chambers where they are established) and appointing authorities to be qualified as data controllers[177]. The arbitral institution determines the purpose and means of the processing of personal data contained in parties' submissions and filings for its own purposes, acting independently of the arbitrators and parties.

With respect to the processing of personal data on the part of an arbitral institution, I should consider whether this institution as a whole should be considered the „controller", or rather its individual members, who determine the purpose and means of processing. In general, where an organised collective entity determines the purposes and means of processing, the point of departure is that the entity as such is the controller, rather than any particular individual natural/physical person who is part of that entity[178]. Thus, it seems that the answer to that question is that it is the institution as a whole which qualifies as the „controller". This is not only due to „the strategic per-

[175] K. Paisley, *It's All About the Data…, op. cit.*, p. 897.

[176] A. Blumrosen, *The Allocation…, op. cit.*, p. 105.

[177] M. Zahariev, *GDPR Issues In Commercial Arbitration And How To Mitigate Them*, 1.06.2021, https://arbitrationbulgaria.com/2021/06/01/gdpr-issues/, accessed: 21.04.2022.

[178] Ch. Kuner et al., *The EU General Data…, op. cit.*, p. 149.

spective of allocating responsibilities", but also „in order to provide data subjects with a more stable and reliable reference entity for the exercise of their rights"[179].

Turning to the status of **arbitrators**, they will also normally act as controllers with respect to the personal data processed by them. As stated in the literature, „the consideration and the final resolution of a dispute, as well as the related data processing, turn arbitrators (similarly to lawyers) into data controllers"[180]. It is inherent in the arbitral tribunal's function – argues K. Paisley – that the arbitrators „control the purpose and means by which they process the documents and evidence presented by the parties, which in turn means that they control the data they receive from the parties and the institution during the course of the arbitration"[181].

Interestingly, some scholars put forward arguments that arbitrators could be considered *processors*, not controllers of personal data. As suggested by A. Blumrosen, „arbitration actors other than the party that made the initial collection of personal data should all be considered processors, and not controllers", as they

> „did not decide to collect the personal data; they did not adopt the procedures for the collection, nor did they have any role in informing the data subject at the time of collection, or in establishing the *purposes and means* of the personal data processing. Rather, the arbitrators received the personal data from the parties, or from party counsel, with a precise mission that is arguably far removed from the control and the processing of data: to use the data (including any personal data provided) for the sole purpose of understanding the parties' factual and legal arguments, and to thereafter draft and issue an award"[182].

While this approach is understandable from the perspective of efficiency of arbitral proceedings, I do not believe that it is likely to be shared by the Court of Justice or the supervisory authorities. Primarily, because the central element of the definition of processors is the processing of personal data *on behalf* of the controller. It would be difficult to justify the view that arbitrators or arbitral

[179] Working Party 29, *Opinion 01/2010 on the Concepts of „Controller" and „Processor"*, 16.02.2010, WP 169, p. 15.

[180] M. Zahariev, *GDPR Issues..., op. cit.*

[181] K. Paisley, *It's All About the Data..., op. cit.*, p. 898.

[182] A. Blumrosen, *The Allocation..., op. cit.*, p. 104.

institutions process personal data on somebody's behalf (other than their own). Data processors must conclude a contract with the controller, in which they undertake to process personal data „only on documented instructions from the controller"[183], which seems inappropriate in the relationship of an independent arbitrator with a party.

Also, there is a risk of abuses in the author's proposal that it should be the party's obligation to „limit, redact, anonymize or pseudonymize the data so that only personal data required for the purposes of the arbitration is sent to the arbitrators"[184], in particular the risk of redacting materially relevant parts of the evidence under the guise of pseudonymization etc. At the same time, one cannot help but agree that requiring arbitrators to contact any person whose personal data is processed, but was not collected by the arbitral tribunal itself, in fulfilment of Art. 14 of the GDPR, may turn out to be in many instances unworkable. It seems that this issue may currently only be resolved by appropriate national legislation enacted under Art. 23 of the GDPR, limiting data subject's rights in order not to impose unduly burdensome obligations on the participants of arbitral proceedings.

The **parties** to the arbitral proceedings, for example by submitting their pleadings or offering evidence containing personal data, also become data controllers. Importantly, parties will very often act as initial data controllers, i.e., entities that initially collected personal data.

The **external counsel**, whose function is to represent the parties and to decide how to present their case based on the evidence, will also typically act as a data controller, given that they determine how and why to process that data[185].

The list of the people and entities mentioned in this chapter includes arguably the most noticeable and important participants of arbitration, but does not exhaust all of the possible controllers in the arbitration setting. Expert witnesses, tribunal secretaries, even translators or assistants – virtually any participant of the proceedings may qualify as a controller.

[183] GDPR, Art. 28(3)(a).

[184] A. Blumrosen, *The Allocation..., op. cit.*, p. 104.

[185] K. Paisley, *It's All About the Data..., op. cit.*, p. 895.

Due to the flexibility of the GDPR terms and the fact-specific approach, it should be no surprise that it is impossible to „pre-assign" data protection roles to arbitration practitioners. As summarised in the scholarship, „the principal data controller is the party, which has collected the data in the normal course of its business from its clients and vendors and is squarely responsible for that data under the GDPR. But counsels and arbitrators may also be controllers, even though they did not initially collect the data, because to perform their respective functions they have broad discretion and professional independence to decide how certain personal data produced in the proceeding should be used"[186].

iv. Joint controllership in arbitration

Are arbitrators forming the same tribunal joint controllers under Art. 26 of the GDPR? It is a complex question. Joint controllership occurs:

> „where two or more controllers jointly determine the purposes and means of processing"[187].

The consequence of joint controllership is that the controllers must, in a transparent manner, determine their respective responsibilities for compliance with the obligations under the GDPR[188]. In particular, the joint controllers must conclude an arrangement reflecting the respective roles and relationships of the joint controllers vis-à-vis the data subjects; the „essence" of the arrangement should be made available to data subjects[189]. This arrangement does not need to be concluded only when the respective roles and relationships of the joint controllers vis-à-vis the data subjects[190]. Importantly, data subjects may exercise their rights against any of the joint controllers, irrespective of their arrangement[191].

[186] A. Blumrosen, *The Allocation..., op. cit.*, p. 99.

[187] Ibid.

[188] GDPR, Art. 26.

[189] GDPR, Art. 26(1-2).

[190] GDPR, Art. 26(1).

[191] GDPR, Art. 26(3).

Some believe that arbitrators acting within one arbitral tribunal do not qualify as joint controllers[192]. They suggest that although, to a certain extent, the arbitrators in a panel pursue the same ultimate goal – to consider and to resolve the dispute referred to them – they also have a significant degree of independence, including with regard to the means used for the processing[193]. In addition, arbitrators are usually subject to different regulations (e.g. compliance, tax, accounting regulations, etc.). Thus, it was remarked that without further guidance and clarifications from either the national supervisory authorities or the European Data Protection Board, the benefits of declaring the arbitrators as joint controllers seem rather doubtful, as they must conclude an arrangement regarding their mutual responsibilities and inform the concerned subjects about the substantial parts thereof[194].

Would qualifying arbitrators as joint controllers be in line with the language of Art. 26(1) of the GDPR, which requires that the controllers act „jointly" in determining the purposes and means of processing? In general terms, the arbitrators process the data for the same purpose, utilizing the same means, with the common ultimate goal – issuing a final, binding award. They do not engage in processing activities for their own purpose, but rather to realize the function of the arbitral tribunal which they are a part of.

It is important to note that participation in the joint determination may take different forms and does not have to be equally shared[195]. As further explained by the CJEU:

> „the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case"[196].

Thus, it would seem that the situation of joint controllership could arise in numerous instances in cases of a multi-arbitrator tribunal. If, for example, processing concerns personal data contained in

[192] M. Zahariev, *GDPR Issues..., op cit.*

[193] Ibid.

[194] Ibid.

[195] Working Party 29, *Opinion 01/2010 on the Concepts of „Controller" and „Processor"*, 16.02.2010, WP 169, p. 19.

[196] Judgment of the Court of Justice of 29.07.2019, C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, para. 70.

the parties' submission (e.g., statement of claim and statement of defence), which is then processed by the tribunal in order to issue an award, it would be difficult to find that there was no collective determination of the purposes and means of processing.

What also deserves some attention is whether the arbitrators could be considered „joint controllers" with the arbitral institution. Given the high degree of interconnectedness between the arbitral tribunal and the arbitral institution, I believe that such a determination could be legally justified, at least with respect to some processing activities. Thus, if a party submits its statement of claim to the arbitral institution, which is then shared with the arbitrators, I do not see a reason why both these entities could not be considered joint controllers with regard to personal data contained in said submission. That assessment is further reinforced by the CJEU's flexible approach to joint controllership. For instance, the administrator of a Facebook fan page was found to be a joint controller with Facebook[197]; moreover, due to the fact that a company has inserted a Facebook plug-in (a „Like" button) on its website, it was a joint controller with Facebook as the button caused the browser of a visitor to that website to request content from the provider of that plug-in (i.e., Facebook)[198].

Therefore, in my view, it is permissible for the arbitral institution and arbitrators to determine their individual responsibilities for compliance with GDPR obligations, including by concluding an arrangement between them. This could be beneficial for data subjects as they would be provided with a clearer picture of the allocation of responsibilities under the Regulation.

c. Data processors in arbitral proceedings

Another important actor in the field of the GDPR is a „**processor**". This term means:

> „a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"[199].

[197] Judgment of the Court of Justice of 5.06.2018, C-210/16, *Wirtschaftsakademie*, ECLI:EU:C:2018:388.

[198] *Fashion ID*, paras. 83-84.

[199] GDPR, Art. 4(8).

The „processor" is one of the principal actors in the operationalisation of data protection law[200]. Its role is inextricably linked to that of „controller" in the sense that the former results from a delegation or „outsourcing" of tasks determined by the controller[201]. The delegation of processing activities from the controller to data processors requires certain conditions to be met:

i. the data processor acts under the instruction of a data controller in undertaking their tasks;
ii. the data processor is not responsible for deciding on the purposes and means of the data processing; and
iii. the data processor is retained under a data processing agreement allowing the data controller to direct the processing and stop it at any time[202].

Are there any participants of the arbitral process that could qualify as „processors"? Some believe that it is unlikely that participants of the arbitral proceedings – e.g., the arbitrators – act as processors, because they still control the purpose and means of data processing[203]. I agree that arbitrators would not normally qualify as processors. It is important to note that the controller–processor relationship is essentially one of subservience – i.e., the processor must obey the dictates of the controller regarding the purposes and means of the processing[204]. As follows from Art. 28(2), the processor shall not engage another processor without prior specific or general written authorisation of the controller. In the arbitration context, both the arbitrators and the arbitral institution independently determine the specific purposes of data processing. There is no subordination between the participants.

However, this does not mean that the relationship controller-processor is unlikely to ever occur in the arbitration context. Examples given in the literature include:

[200] Ch. Kuner et al., *The EU General Data…, op. cit.*, p. 160.

[201] Ibid.

[202] ICCA, IBA, *The ICCA-IBA Roadmap…, op. cit.*, p. 10.

[203] Ibid.

[204] Ch. Kuner et al., *The EU General Data…, op. cit.*, p. 161.

- entities such as translators or transcribers, to whom participants delegate the performance of a processing activity[205];
- data analyst and e-discovery professionals, who conduct the initial data review before it is provided to counsel, will also act as data processors[206]; or
- a party producing evidence on the order of an arbitral tribunal[207].

While the given examples could potentially give rise to a controller-processor relation, it is important to bear in mind that the formation of such a relation requires specific conditions to be met. In particular, the processor's activities must be governed

> „by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller"[208].

Importantly, when the conditions set forth in the Regulation are not met, the person or entity involved in the determination of purposes and means of processing will not qualify as processor and will remain a controller, as explicitly provided in Art. 28(10). Thus, an entity carrying out a processing activity on behalf of a controller remains a controller, unless other requirements are fulfilled. From a practical standpoint, it seems unlikely that arbitral tribunals would be willing to conclude complex data processing agreements required under the GDPR to allow parties to act as processors and thus limit their obligations under the Regulation.

d. Data subjects in the arbitral proceedings and their rights

[205] L. Ben Ammar, *Data Protection Obligations in International Arbitration*, 4.05.2021, https://www.gtlaw.com/en/insights/2021/5/data-protection-obligations-in-international-arbitration, accessed: 21.04.2022.

[206] K. Paisley, *It's All About the Data…, op. cit.*, p. 896.

[207] G.N. Ramani, *One size…, op. cit.*, p. 618.

[208] *See* GDPR, Art. 28(3).

This part of the chapter will try to identify the persons that are likely to appear as data subjects in the arbitral setting. It will not provide an exhaustive overview of the data subjects' rights as such rights are generally universal for all data subjects[209].

Although there is no direct definition of the term „data subject", on the basis of the GDPR one can establish that this term refers to a natural person, who is identified or identifiable pursuant to some information (which is then considered „personal data").

Virtually any participant of the arbitral process may act as a data subject. Employees whose emails are processed by a party will be the data subject. A witness's written testimonies containing personal data will be data subjects. Candidates for arbitral nomination analysed by the party's counsel will be data subjects. Party's contractors (natural persons) whose bank account numbers are submitted as evidence will be data subjects.

The basic rights of the data subject include the following:

1) the right of access and to obtain a copy of the personal data being processed[210];
2) the right to request modification of their data, including the correction of errors and the updating of incomplete information[211];
3) the right to withdraw consent if consent was the basis for processing[212];
4) the right to object to processing where the lawful basis relied upon is a legitimate interest, in which case the controller should demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject[213];
5) the right to erasure – also referred to as the right to deletion or the right to be forgotten – allows a data subject to request, under certain circumstances, that their personal data be erased[214].

[209] Thus, the reader can be referred to general works on the data subjects and their rights under the GDPR. *See* P. Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer 2017, p. 141-187.

[210] GDPR, Art. 15.

[211] GDPR, Art. 16.

[212] GDPR, Art. 7(3).

[213] GDPR, Art. 21.

[214] GDPR, Art. 15(4).

e. Conclusions

In arbitral proceedings, everyone has their permanently assigned role: arbitrators issue orders and awards, parties present their submissions and offer evidence, witnesses give their testimonies, etc. This approach, however, has very little to do with the GDPR's *modus operandi*. From the data protection perspective, the landscape of rights and obligations changes like in a kaleidoscope – a party may act as a data controller with respect to, e.g., their employee's data, while the employees are data subjects in relation to, e.g., arbitral tribunals. An expert witness is a data controller with respect to the documents shared with them to prepare an expert report, while being the data subject while their background is questioned by the party's counsel.

The configurations of data processing in the context of arbitration could be multiplied and it would be difficult, if not impossible, to predetermine which entity will fulfil which role from the GDPR perspective. The flexibility of the Regulation's concepts and the attention it gives to each processing activity makes it necessary to take into account the particular circumstances of each processing and the actors involved. As noted, „the broadly-worded GDPR principles, and the lack of arbitration-specific guidance, require a complicated fact-specific assessment of GDPR in each arbitration"[215]. This includes the allocation of data protection roles among the participants of the arbitral proceedings.

When in doubt, it may be a safe bet to take guidance from the goal of the GDPR, which is to „effectively protect the fundamental rights and freedoms of natural persons with regard to the processing of their personal data"[216], while at the same time bearing in mind that the right to the protection of personal data „is not an absolute right and must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality"[217].

[215] A. Blumrosen, *The Allocation..., op. cit.*, p. 95

[216] A. Blumrosen, *The Allocation..., op. cit.*, p. 93.

[217] GDPR, recital 4.

PRINCIPLES OF THE PROCESSING OF PERSONAL DATA IN ARBITRATION

a. Introduction

Participants of any arbitration governed by the GDPR, who take part in the processing of personal data, must comply with various obligations imposed by the Regulation. A key part of them was enshrined in Article 5(1), which establishes the principles governing the processing of personal data. Any discussion on the influence of the Regulation on arbitration proceedings would be incomplete without addressing how these principles „translate" to the particular setting of arbitration and what are their practical implications for the course of the dispute resolution process.

There are six main principles – or, in some cases, groups of principles, relating to the processing of personal data under the GDPR. These include:

- lawfulness, fairness and transparency (Art. 5(1)(a));
- purpose limitation (Art. 5(1)(b));
- data minimisation (Art. 5(1)(c));
- accuracy (Art. 5(1)(d));
- storage limitation (Art. 5(1)(e));
- integrity and confidentiality (Art. 5(1)(f));
- accountability (Art. 5(1)(g)).

This set of principles has not been significantly modified since the first international instruments in the field of data protection were adopted, in particular the 1980 OECD Guidelines and the Convention 108 of 1981. It is believed that „more than 30 years of practical application have proven these principles to be sound"[218]. I will now look separately at each of these principles to discuss what is their meaning and scope, as well as their role in arbitral proceedings.

[218] W. Kotschy, *The Proposal for a new General Data Protection Regulation – Problems Solved?*, International Data Privacy Law 2014, vol. 4(4), p. 277.

b. Lawfulness, fairness and transparency

Pursuant to Art. 5(1)(a) of the GDPR:

> „personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject".

The requirement that data processing must be **lawful** essentially means that it respects all applicable legal requirements[219]. The condition of ensuring the lawfulness of data processing means primarily the need to meet the prerequisites for the lawfulness of data processing listed in Articles 6 and 9 and to ensure compliance with other provisions on personal data protection[220]. Accordingly, to be considered as lawful, the processing of personal data should be in accordance with the law, should pursue a legitimate purpose and be necessary and proportionate in a democratic society in order to achieve that purpose[221].

The notion of **fairness** in data protection law aims to ensure that personal data is processed only in ways that data subjects would reasonably expect[222]. It also entails that personal data cannot be used in a manner that has an unjustified adverse effect on the data subject[223]. Fair processing implies that data have not been obtained or otherwise processed through unfair means, by deception or without the data subject's knowledge[224].

In the arbitration context, fairness triggers the question of whether the data subject, whose data is processed during the arbitration, could have anticipated the processing in view of how it was

[219] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 315.

[220] A. Nerka, *Art. 5* [in:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, M. Sakowska-Baryła (ed.), Warsaw 2018, para. 2.

[221] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 315.

[222] ICCA, IBA, *The ICCA-IBA Roadmap..., op. cit.*, p. 15.

[223] Ibid.

[224] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 315.

collected and the notices given, as well as whether processing will have adverse effects on the data subject that are not justified by the needs of the processing for the arbitration[225].

Transparency of processing was explained in recital 39, which states that „it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed". The principle of transparency requires data subjects to be provided with notice in plain language about the processing of their personal data and the purpose for the processing[226]. The notice requirement is described in Art. 13-14, which requires the controller to provide the data subject with certain information whenever their personal data is collected and obtained.

The principle of transparency may be particularly difficult to reconcile with arbitration, one of the main features of which is confidentiality. For example, in line with Art. 13-14 of the Regulation, data subjects have to be notified when their data is processed by a law firm preparing to submit a claim. This, however, may be contrary to the party's interests and to the confidentiality of the process. The exception to the transparency provided in the GDPR includes the need for confidentiality, which, however, is limited to an obligation of „professional secrecy"[227], which may turn out insufficient in arbitration. As noted in the scholarship, this standard will typically not be met by arbitral confidentiality generally, although it may apply to counsel who is subject to legal privilege and to the arbitrator's duty of confidentiality"[228].

c. Purpose limitation

As follows from Art. 5(1)(b):

> „personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes

[225] ICCA, IBA, *The ICCA-IBA Roadmap..., op. cit.*, p. 15.

[226] Ibid., p. 30.

[227] Art. 14(5)(d).

[228] K. Paisley, *It's All About the Data..., op. cit.*, p. 908.

or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes".

This principle, called the „purpose limitation principle", requires data to be collected for specified, explicit and legitimate purposes (the „purpose specification" dimension) and not further processed in a manner that is incompatible with those purposes (the „compatible use" dimension)[229]. The principle of purpose limitation can be further described as requiring the following:

- the purposes for processing personal data should be determined from the very beginning, at the time of the collection of the personal;
- the purposes for processing must be unambiguous and clearly expressed instead of being kept hidden;
- the purposes must be legitimate, which means that they may not entail a disproportionate interference with the rights, freedoms and interests at stake, in the name of the interests of the data controller[230].

This principle also implies that the controller may perform on these data all the operations that may be considered to be compatible with the initial purposes[231]. Article 6(4) of the Regulation sets out the criteria for the determination of whether processing for a purpose other than the initial purpose is to be deemed compatible with this initial purpose.

The principle of purpose limitation is related to the transparency requirement, in that the data subject should receive a notice, identifying the purpose of the processing of their personal data. The subsequent processing activities must then be limited to the purpose that was notified to the data subject[232].

In the arbitration context, if personal data is processed by the participants of arbitral proceedings who did not originally collect the data, which is often the case, the possibility of processing for the

[229] Ch. Kuner et al., *The EU General Data…, op. cit.*, p. 316.

[230] Ibid.

[231] Ibid.

[232] ICCA, IBA, *The ICCA-IBA Roadmap…, op. cit.*, p. 22.

purpose of the arbitration must either have been included in the original notice given to the data subject or be compatible with the purpose identified therein[233].

It is important to note that Member States can derogate from the application of the purpose limitation. In Germany, for example, controllers are permitted to process personal data for a purpose other than the one for which the data was collected where the legal claims derogation applies[234].

d. Data minimisation

In Art. 5(1)(c) of the GDPR, it was enshrined that:

> „personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

The principle of data minimisation is considered „fundamental to modern data protection regimes"[235]. In the context of arbitral proceedings, this principle requires all its participants to ensure that the amount and type of personal data processed is adequate, relevant and limited to what is necessary for the lawful purpose of the processing (i.e., preparing a case for arbitration, prosecuting, defending against, or deciding a claim, administering the proceedings, or retaining data in relation to the arbitration after completion of the proceedings)[236]. Adherence to this principle may require data scrubbing for relevant data and elimination of sensitive data as a first step before the data is even processed for the arbitration, and potentially pseudonymization of the relevant data where feasible[237].

It is important to note that the principle of data minimisation applies in all stages of arbitration. A particularly important phase of arbitration from the perspective of the principle of data minimisation is document production, which is the procedural tool by which a party or the tribunal can re-

[233] Ibid.

[234] Ibid.

[235] Ibid., p. 20.

[236] Ibid., p. 21.

[237] K. Paisley, *It's All About the Data…, op. cit.*, p. 902.

quest (and order) the production of documents in possession of the other party, allowing them to obtain further evidence to substantiate their case[238].

This principle will be relevant in the selection, production and disclosure of documents[239]. It prohibits the processing of an excessively large amount of personal data (asking an employee for her complete medical file to assess her capacity to work, for example)[240]. Thus, the requests for document production should be rejected or limited by the arbitral tribunal on the ground of data protection laws if they went beyond what is necessary to establish the relevant facts.

Moreover, it seems that the data controllers in arbitration should not allow for the processing of relevant facts, if this would entail a disproportionate interference in the data subject's rights and interests[241]. For example, it may be inappropriate to request a full history of a witness medical history or drug consumption, even if such information could potentially be relevant for the assessment of his or her credibility.

e. Accuracy

In accordance with Art. 5(1)(d):

> „personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay".

The requirement that data be accurate and, where necessary, kept up to date, was already present in the DPD and in Convention 108, and has been maintained in the GDPR[242]. The legislation does not specify the criteria for assessing reasonable efforts by the controller, however, it can be pre-

[238] J. Touzet, C. Gambarini, *Document Production*, 24.12.2021, Jus Mundi, https://jusmundi.com/en/document/wiki/en-document-production, accessed: 21.04.2022.

[239] ICCA, IBA, *The ICCA-IBA Roadmap..., op. cit.*, p. 21.

[240] Ch. Kuner et al., *The EU General Data..., op. cit.*, p. 318.

[241] Ibid.

[242] Ibid.

sumed that it is about taking reasonable steps to erase or rectify data at the request of the data subject or on the basis of information in its possession obtained from reliable external sources[243].

It is important to note that the scope of the obligations stemming from this principle will to a considerable extent be dependent on the purpose of the processing. For example, in arbitration, there is generally no obligation to update all personal data in the record if they refer to facts which occurred in the past, unless it becomes clear that the facts in the record are wrong or misleading; however, when it comes to light that personal data is incorrect or misleading, reasonable steps should be taken to promptly correct or erase it[244]. This principle does not require the controller to continuously monitor the accuracy and timeliness of all data it processes on its own initiative[245].

f. Storage limitation

As provided for in Art. 5(1)(e) of the GDPR:

> „personal data shall be kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject".

Data retention is an area that is considered to be difficult to reconcile with arbitration[246]. The WP29 has taken a restrictive view that unlimited retention of data for the purpose of later disputes, until the statute of limitations expires, may be unlawful[247]. This runs counter to the practice of arbitration practitioners to retain access to the factual record. K. Paisley believes that „applying

---

[243] M. Sakowska-Baryła, *Ogólne rozporządzenie..., op. cit.,* para. 7.

[244] ICCA, IBA, *The ICCA-IBA Roadmap..., op. cit.*, p. 26.

[245] M. Sakowska-Baryła, *Ogólne rozporządzenie..., op. cit.,* para. 7.

[246] K. Paisley, *It's All About the Data..., op. cit.*, p. 906.

[247] Working Party 29, *Working Document 1/2009 on pre-trial discovery for cross border civil litigation*, 11.02.2009, WP 158, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf, accessed: 22.04.2022, p. 12.

this logic to arbitration implies that the need to have access to data for a later arbitration is unlikely to be a sufficient basis on its own to retain data longer than would otherwise be reasonable"[248].

g. Integrity and confidentiality

Article 5(1)(f) expresses the principles of integrity and confidentiality of the processing of personal data. Pursuant to it:

> „personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

This principle, generally speaking, refers to the security of the processed data, as „the crucial requirement of security that is now included in the list of fundamental principles of data protection"[249]. It is the duty of the controller and the processor to implement such technical and organisational measures[250]. Article 32 of the GDPR also lists examples of such measures (e.g. the pseudonymisation and encryption of personal data). Deciding what security measures are „appropriate" requires consideration of the potential risk to data subjects, the existing information security measures of the participants of the proceedings, and what physical and technical measures are appropriate given the risks to the data subjects[251].

This principle is further elaborated on in Art. 32 of the Regulation, which proclaims that the analysis of whether technical and organisational measures ensure the data security should take into account: the state of the art, the costs of implementation and the nature, scope, context and purposes of processing; as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

---

[248] K. Paisley, *It's All About the Data…, op. cit.*, p. 906.

[249] Ch. Kuner et al., *The EU General Data…, op. cit.*, p. 320.

[250] GDPR, Art. 32(1).

[251] ICCA, IBA, *The ICCA-IBA Roadmap…, op. cit.*, p. 26-27.

The assessment of the appropriate level of security should include the risks that are presented by processing, in particular from an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed[252].

A particularly important component of the data security principles are the obligations stemming from any cases of a data breach. Data controllers are required to notify the supervisory authorities in case of a data breach that is „likely to result in a risk to the rights and freedoms of the data subject" within 72 hours of their discovery of the breach[253]. The data subjects themselves must also be notified of the breach if the risk to personal data and data subjects from a breach is considered to be „high"[254]. The EU Working Party has indicated that a data controller is deemed to become aware of a breach when it has a „reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised"[255].

Implementation of the integrity and confidentiality principle is in line with international efforts to increase cybersecurity in international arbitration. These efforts include, for example, the adoption of the Protocol on Cybersecurity in International Arbitration – a set of guidelines, which provides guidance for counsel, arbitrators, and institutions, and optional protocols that can be adopted by parties to an arbitration[256]. The Protocol presents the view that „information security and data protection issues are closely connected" as „it is typical for data protection law and regulations to mandate, among other things, that persons processing personal data implement reasonable information security measures"[257].

h. Accountability

The last principle relating to the processing of personal data – accountability – is enshrined in Art. 5(1)(g) of the GDPR. It mandates that the controller shall be responsible for, and be able to dem-

[252] GDPR, Art. 32(2).

[253] GDPR, Art. 33-34.

[254] GDPR, Art. 34.

[255] Working Party 29, *Guidelines on Personal data breach notification under Regulation 2016/679*, 3.10.2017, p. 11.

[256] *The 2020 Protocol on Cybersecurity in International Arbitration*, adopted by the International Council for Commercial Arbitration, the New York City Bar Association and the International Institute for Conflict Prevention and Resolution, https://www.arbitration-icca.org/cybersecurity-international-arbitration-icca-nyc-bar-cpr-working-group, accessed: 22.04.2022.

[257] Ibid., p. ix.

onstrate compliance with the principles relating to the processing of personal data, listed in Art. 5(1).

The accountability principle essentially requires data controllers to take personal responsibility for data protection compliance and record the measures they take to comply with their data protection obligations[258]. Demonstrating compliance requires, in particular, maintaining a record of processing activities by each controller and processor[259].

From the practical standpoint, it is advisable for the participants of arbitration to document all measures and decisions taken regarding compliance with the GDPR – in particular, the lawful basis relied on for data processing/third country transfers of data and any legitimate interests analysis, etc.[260] Importantly for arbitrators and smaller law firms, the strict record-keeping obligations do not apply to small and medium-sized enterprises (employing fewer than 250 persons), but all those concerned should be mindful of the exceptions to this exception, set out in Art. 30(5)[261].

A data protection protocol can play an important part in documenting compliance; however, it may have to be shared with the authorities[262]. It was proposed that as a matter of good practice – although not explicitly required of independent controllers – arbitrators and arbitral institutions should consider entering into a mutual agreement regulating the issues on how data protection within the tribunal shall be ensured[263]. This agreement could be used as documentary evidence and proof that the GDPR requirements have been met and would enable arbitrators acting as controllers to demonstrate compliance with the GDPR principles[264]. The agreement should at minimum regulate aspects such as: what personal data will be collected and otherwise processed; what types of the data subjects the personal data relates to; for what purposes and on what legal ground under GDPR the data will be processed; retention periods and territory of the processing;

[258] ICCA, IBA, *The ICCA-IBA Roadmap..., op. cit.*, p. 32.

[259] GDPR, Art. 30(1-2).

[260] Ibid., p. 32.

[261] K. Paisley, *It's All About the Data..., op. cit.*, p. 852.

[262] ICCA, IBA, *The ICCA-IBA Roadmap..., op. cit.*, p. 33.

[263] Ibid.

[264] Ibid.

what the main responsibilities of the arbitrators and institutions as independent controllers will be[265].

i. Rules concerning data transfer

The imposition of restrictions on data transfer is one of the most obvious ways that data protection laws influence international arbitrations[266]. Given that such proceedings involve parties from different jurisdictions, it is important to take notice of regulations intended to restrict the transfer of data to third countries. An example of the jurisdictional diversity of international arbitration was provided by E. Mazetova, who explains 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"[267].

In recital 101 of the GDPR it was noted that „flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation". This transfer, however, should not undermine the level of protection of data privacy[268]. A general rule is that the transfer of personal data to a third country (or international organisation) is only permissible if conditions laid down in Chapter V of the GDPR are met[269]. There are four legal bases for a lawful transfer of personal data under the GDPR that are likely to find application in the context of arbitration:

1) on the basis of an adequacy decision (Art. 45);
2) on the basis of „appropriate safeguards" (Art. 46);

---

[265] M. Zahariev, *GDPR Issues…, op. cit.*

[266] ICCA, IBA, *The ICCA-IBA Roadmap…, op. cit.*, p. 11.

[267] E. Mazetova, *Data Protection Regulation and International Arbitration: Can There Be Harmonious Coexistence (with the GDPR Requirements Concerning Cross-Border Data Transfer)?,* Legal Issues in the Digital Age 2021, vol. 2, p. 28.

[268] GDPR, recital 101.

[269] GDPR, Art. 44.

3) on the basis of a judgment of a court of tribunal or a decision of an administrative authority of a third country (Art. 48);
4) on the basis of a derogation (Art. 49).

Transfer on the basis of an **adequacy decision** may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection[270]. In such cases, a particular transfer does not require any specific authorisation. The appropriate adequacy decisions have been issued by the Commission for the following countries (or territories): Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay[271]. An adequacy decision in favor of a country means that the EU Commission, after scrutinizing 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[272].

The adequacy decision is not a permanent guarantee – 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 pertaining to invalidation of the data protection regimes agreed to between the EU and the USA: the U.S.-EU Safe Harbor Framework and the EU-U.S. Privacy Shield[273].

In the first ruling, issued before the GDPR has been adopted, the Court found that the adequacy decision for the United States (U.S.-EU Safe Harbor) was invalid[274]. First, the Commission did not state in the decision that the United States in fact ensured an adequate level of protection by reason of its domestic law or its international commitments. Second, the decision infringed the national supervisory authorities' powers to examine, with complete independence, claims concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to them.

---

[270] GDPR, Art. 45(1).

[271] *Adequacy decisions,* https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, accessed: 31.05.2022.

[272] E. Mazetova, *Data Protection Regulation..., op. cit.,* p. 30.

[273] Ibid.

[274] Judgment of the Court of Justice of 6.10.2015, C-362/14, *Schrems*, ECLI:EU:C:2015:650.

Subsequently, the U.S.-EU Safe Harbor was replaced by the EU-US Privacy Shield[275]. However, in July 2020, the CJEU has found the Commission Implementing Decision 2016/1250 to be invalid in the *Schrems II* ruling[276]. The reason for this ruling was that the US law granted rights of access to private data for USA public authorities; this meant that the necessary data protection could not be ensured[277]. The CJEU concluded that the US surveillance laws (principally Section 702 of Foreign Intelligence Surveillance Act and Executive Order 12333) do not limit or effectively oversee public authorities' access to personal data; and the Privacy Shield does not grant EU individuals actionable and effective rights before the courts against such public authorities. To the latter point, the CJEU held that the Privacy Shield Ombudsman cannot effectively remedy these deficiencies[278].

Recently, in March 2022, the EU and the US announced that they agreed „in principle" to a new framework for cross-border data transfers; the process is expected to be finalised by the end of 2022[279].

Transfer on the basis of „**appropriate safeguards**" is permissible in the absence of the adequacy decision. Under this legal ground, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available[280]. The Regulation lists several appropriate safeguards, for example a legally binding and enforceable instrument between public authorities or bodies or standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2). When such appropriate safeguards are provided, the transfer does not require any specific authorisation from a supervisory authority[281]. Importantly from the arbitration perspective, one of such safeguards are „contractual clauses between the controller or processor

[275] Commission Implementing Decision 2016/1250 of 12.06.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L 207/1.

[276] Judgment of the Court of Justice of 16.07.2020, C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems,* ECLI:EU:C:2020:559.

[277] E. Mazetova, *Data Protection Regulation..., op. cit.,* p. 31.

[278] *Schrems II landmark ruling: A detailed analysis*, https://www.nortonrosefulbright.com/en/knowledge/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis, accessed: 31.05.2022.

[279] N. Lomas, *EU-US data transfers deal could be finalized by end of year, says bloc*, 12.04.2022, https://techcrunch.com/2022/04/12/eu-us-data-transfers-deal-expected-timeline/, accessed: 31.05.2022.

[280] GDPR, Art. 46(1).

[281] GDPR, Art. 46(2).

and the controller, processor or the recipient of the personal data in the third country or international organisation". The transfer on the basis of contractual clauses, however, requires additional authorisation from the competent supervisory authority[282].

Under Art. 48, a transfer may be authorised on the basis of a „**judgment of a court or tribunal and any decision of an administrative authority of a third country**" requiring a controller or processor to transfer or disclose personal data. This judgment or decision, however, may only be recognised or enforceable, if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State[283]. It is believed that arbitral tribunal would qualify as a competent requesting authority for the purpose of this provision[284]. Currently, however, the 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[285].

Transfer on the basis of a **derogation for specific situation** is permissible in the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46. The GDPR provides a list of seven legal grounds which allow for the transfer, from which the most appropriate in the context of arbitration refers to a transfer that is necessary for the „establishment, exercise or defence of legal claims"[286]. This view is also shared by the VIAC, whose Privacy Statement reads: „[d]ata will be transferred to other persons as far as it is necessary to perform administration of the proceedings. This includes that data may also be transferred outside the EU or European Economic Area. The legal basis for the transmission is contained in Art 49 GDPR: the transfer is necessary for the establishment, exercise or defence of legal claims"[287].

[282] GDPR, Art. 46(3).

[283] GDPR, Art. 48.

[284] E. Mazetova, *Data Protection Regulation..., op. cit.*, p. 40.

[285] Ibid., p. 43.

[286] The legal claims exception is most likely to constitute a justified legal basis for the transfer of data in the context of international arbitration. *See* GDPR *Issues In International Arbitration*, 10.08.2020, https://www.paulweiss.com/practices/litigation/international-arbitration/publications/gdpr-issues-in-international-arbitration?id=37691, accessed: 23.04.2022.

[287] VIAC, *Arbitration Privacy Policy,* https://www.viac.eu/en/privacy-statement, accessed: 23.04.2022.

Additionally, if none of the derogations is applicable, a party may rely on its „compelling legitimate interests" as a basis for the transfer, which, however, is a high threshold to meet, and also requires notification to both the data subjects and the supervisory authority, which means that it is unlikely to be often applied in practice in arbitration[288].

[288] L. Ben Ammar, *Data Protection..., op. cit.*

CONCLUSIONS

Interference of data protection laws in the dispute resolution process imposes upon its participants numerous obligations, which may seem like an unnecessary, time-consuming hurdle. In reality, however, giving the GDPR the attention it deserves may actually facilitate arbitral proceedings.

First, compliance with the GDPR helps to achieve the goal of the arbitral proceedings, which is to resolve the dispute by rendering an enforceable award. As speculated by some authors, the infringement of the Regulation in the course of arbitral proceedings could potentially lead to the refusal of the enforcement of the award under the New York Convention[289] on the ground of public policy violation[290].

Second, it minimises the risk of abuse of data protection laws, for example, by withdrawing consent for data processing. Any violation of the data subjects' rights could extend the proceedings and risks the involvement of national supervisory authorities or courts, jeopardising the parties' right to obtain a binding award in a just and timely procedure. Resolving data protection issues at an early stage of the proceedings – e.g., during a pre-trial conference or in a procedural order – ensures that they will not disrupt the course of the proceedings during their substantive phase.

Third, compliance with the GDPR protects the arbitration practitioners from severe penalties for infringement of the GDPR, which may amount to EUR 20 million or 4% of an undertaking worldwide annual turnover, whichever is higher, for the most serious offences and half of these figures for others[291].

Fourth, in today's world, where data privacy laws are taken more and more seriously, there seems to be a moral obligation among arbitration practitioners (or lawyers more broadly) to ensure that the highest standards of personal data protection are provided to the participants of the dispute resolution process. Simply speaking, it is a matter of professional standards to afford other people the appropriate respect for their privacy, including personal data rights. Thus, efforts from leading

[289] United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards, New York, 10.06.1958.

[290] A. Blumrosen, *The Allocation..., op. cit.*, p. 107-109.

[291] GDPR, Art. 83(4-5).

arbitral institutions to ensure GDPR compliance should be welcomed. For example, the ICC Court of Arbitration in its note has required the arbitral participants to ensure that the GDPR is followed, e.g., by anonymisation, pseudonymisation, use of notices and appropriate information security measures[292]. This is definitely a positive development and other arbitral institutions should follow suit[293].

Arbitration has not been exempted from obligations imposed by the GDPR. Personal data processed in the course of arbitral proceedings is protected. Arbitration, in all likelihood, falls under the material scope of the GDPR, although this matter may prove to be a point of contention between arbitration practitioners and data protection authorities. Territorially, whether a given processing activity is governed by the Regulation depends primarily on the location of the controller or processor's establishment. While the GDPR provides a sufficient legal basis to cover most, if not all, processing activities involving personal data in arbitration, the question whether the rights of the data subjects are adequately and effectively safeguarded will depend on persistent enforcement of these rights by the data subjects and adequate oversight of supervisory authorities.

There are also some legal issues that may prove to be an obstacle to a consistent and firm application of the GDPR in the context of arbitration. While many legal bases set forth in the Regulation could potentially justify processing of personal data in arbitration, there is no single basis covering all processing activities. The lack of an express legal ground applicable in the context of arbitral proceedings may pose practical problems. If the courts or supervisory authorities question the applicability of the „legitimate interests" legal basis – which seems the most suitable for arbitration – it may turn out necessary to adopt an additional legal ground, justifying processing in the context of alternative dispute resolution mechanisms. In the literature it was proposed to amend Art. 6 of the GDPR to include: „[t]he processing of personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in any other judicial or quasi-judicial proceedings, arbitrations, mediations, conciliations or other out-of-court proceedings"[294].

---

[292] ICC, *Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration*, 1.01.2021, https://iccwbo.org/publication/note-parties-arbitral-tribunals-conduct-arbitration/, accessed: 25.04.2022.

[293] *See, e.g.,* VIAC, *Arbitration Privacy Policy,* https://www.viac.eu/en/privacy-statement, accessed: 25.04.2022.

[294] G.N. Ramani, *One size…, op. cit.*, p. 629.

Alternatively, it would also be possible to exempt the arbitral tribunals from some GDPR-related obligations in order to adapt the law to the reality of dispute resolution proceedings, similarly to the judicial capacity exemption. For example, Art. 55 – removing courts from the competence of supervisory authorities – could be amended to include arbitrators and other quasi-judicial authorities exercising judicial functions[295].

For the time being, national authorities, seeking to maintain their status as „arbitration-friendly" jurisdiction, should consider, preferably under the guidance of the European Data Protection Board, making use of Art. 23 of the Regulation and imposing necessary restrictions on the rights of the data subjects, ensuring that the arbitrators and other participants are able to focus on their substantive roles, while respecting the core of the right to the protection of personal data. Otherwise, the GDPR in the arbitration context may become a dead letter, enforced incidentally in cases of violations, not by voluntary, widespread compliance.

After five years of the GDPR's application, many pressing issues relating to arbitration remain unresolved. In all probability, people's awareness of their data privacy rights will continue to grow, which may lead to more clarity at the intersection of arbitration and data protection. Thus far, both fields remain separate worlds, which, however, are destined to cohabitate. Whether this will be a peaceful coexistence or a clash depends on the willingness of both communities – arbitration and data protection practitioners – to remain flexible and make good faith efforts to meet the needs and demands of each other.

[295] Ibid., p. 629-630.

BIBLIOGRAPHY

Books

Bennet C.J., R*egulating privacy. Data Protection and Public Policy in Europe and the United States*, Cornell University Press 1992

Bielak-Jomaa E., Lubasz D., *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warsaw 2018

Blumrosen A., *The Allocation of GDPR Compliance in Arbitration*, [in:] *International Arbitration and EU Law*, Mata Dona J.R., Lavranos N., Edward Elgar 2021

Born G., *International Arbitration: Law and Practice*, Kluwer Law International 2012

Bygrave L.A., *Data Protection Law. Approaching its Rationale, Logic and Limits*, Kluwer Law International 2002

Ereciński T., Weitz K., *Sąd arbitrażowy*, Warsaw 2008

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* Warsaw 2022

Fouchard Ph., Gaillard E., Goldman B., *Fouchard, Gaillard, Goldman on International Commercial Arbitration*, Kluwer Law International 1999

Kuner Ch., Bygrave L.A., Docksey Ch., and Drechsler L., *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press 2020

Litwiński P., *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warsaw 2021

Platten N., *Background to and History of the Directive*, [in:] *EC Data Protection Directive*, Bainbridge D., London, Butterworths, 1996

Sakowska-Baryła M., *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warsaw 2018

Szumański A., *Arbitraż handlowy* [in:] *System Prawa Handlowego*, t. 8, Warsaw 2015

Van Alsenoy B., *Data Protection Law in the EU: Roles, Responsibilities and Liability*, Intersentia 2019

Voigt P., von dem Bussche A., *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer 2017

Articles

Bantekas I., *Equal Treatment of Parties in International Commercial Arbitration*, International & Comparative Law Quaterly 2020, vol. 69(4).

Bermann G.A., *European Union Law and International Arbitration at a Crossroads*, Fordham International Law Journal 2018, vol. 42

Birnhack M.D., *The EU Data Protection Directive: An engine of a global regime*, Computer Law & Security Review 2008, vol. 24(6)

Huang J., Xie D., *Data Protection Law in Investment Arbitration: Applicable or Not?*, Arbitration International 2021, vol. 37(1)

Kirby M.D., Transborder Data Flows and the „Basic Rules" of Data Privacy, Stanford Journal of International Law 1980, vol. 16

Kotschy W., *The Proposal for a new General Data Protection Regulation – Problems Solved?*, International Data Privacy Law 2014, vol. 4(4)

Mazetova E., *Data Protection Regulation and International Arbitration: Can There Be Harmonious Coexistence (with the GDPR Requirements Concerning Cross-Border Data Transfer)?*, Legal Issues in the Digital Age 2021, vol. 2

Paisley K., *It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration*, Fordham International Law Journal 2018, vol. 41(4)

Ramani G.N., *One size doesn't fit all: the General Data Protection Regulation vis-à-vis international commercial arbitration*, Arbitration International 2021, vol. 37(3)

Słok-Wódkowska M., Wiącek M., *Zgodność dwustronnych umów inwestycyjnych pomiędzy państwami członkowskimi z prawem Unii Europejskiej. Glosa do wyroku TS z dnia 6 marca 2018 r., C-284/16*, Europejski Przegląd Sądowy 2018, vol. 11

Solove D., *Conceptualising Privacy*, California Law Review 2002, vol. 90

Warren S.D., Brandeis L., *The Right to Privacy*, Harvard Law Review 1890, vol. 4.

Case-law

Opinion of Advocate General Maduro of 3.04.2008, C-524/06, Huber, ECLI:EU:C:2008:194

Judgment of the Court of Justice of 29.06.2010, C-28/08 P, Commission v Bavarian Lager, ECLI:EU:C:2010:378

Judgment of the Court of Justice of 9.11.2010, Joined cases C-92/09 and 93/09, Schecke, ECLI:EU:C:2010:662

Judgment of the Court of Justice of 19.04.2012, C-461/10, Bonnier Audio, ECLI:EU:C:2012:219

Judgment of the Court of Justice of 17.10.2013, C-291/12, Schwarz, ECLI:EU:C:2013:670

Judgment of the Court of Justice of 6.11.2013, C-101/01, Lindqvist, ECLI:EU:C:2003:596,

Opinion of Advocate General Sharpston of 12.12.2013, Joined Cases C-141/12 and C-372/12, YS, ECLI:EU:C:2013:838

Judgment of the Court of Justice of 8.04.2014, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland, ECLI:EU:C:2014:238

Judgment of the Court of Justice of 13.05.2014, Google Spain, C-131/12, ECLI:EU:C:2014:317

Judgment of the Court of Justice of 6.10.2015, C-362/14, Schrems, ECLI:EU:C:2015:650

Judgment of the Court of Justice of 9.03.2016, C-398/15, Manni, ECLI:EU:C:2017:197

Judgment of the Court of Justice of 27.09.2016, C-73/16, Puškár, ECLI:EU:C:2017:725

Judgment of the Court of Justice of 19.10.2016, C-582/14, Breyer, ECLI:EU:C:2016:779

Judgment of the Court of Justice of 20.12.2017, C-434/16, Peter Nowak v Data Protection Commissioner, ECLI:EU:C:2017:994

Judgment of the Court of Justice of 10.07.2018, C-25/17, Jehovan todistajat, ECLI:EU:C:2018:551

Judgment of the Court of Justice of 14.02.2019, C-345/17, Buivids, ECLI:EU:C:2019:122

Judgment of the Court of Justice of 29.07.2019, C-40/17, Fashion ID, ECLI:EU:C:2019:629

Procedural Order no. 2 of 29.07.2019, Tennant Energy, LLC (USA) v Government of Canada, PCA Case No. 2018-54

Judgment of the Court of Justice of 9.07.2020, C-272/19, VQ v Land Hessen, ECLI:EU:C:2020:535

Judgment of the Court of Justice of 16.07.2020, C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559

Internet sources

Adequacy decisions, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Ben Ammar L., Data Protection Obligations in International Arbitration, 4.05.2021, https://www.gtlaw.com/en/insights/2021/5/data-protection-obligations-in-international-arbitration

Burianski M., Data Privacy in International Arbitration, 19.10.2018, https://www.whitecase.com/publications/alert/data-privacy-international-arbitration

Court of Justice of the EU, Protection of Personal Data (Fact sheet), July 2020, https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf

European Commission, What constitutes data processing?, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en

European Commission, What is Personal Data?, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 12.11.2019

GDPR Issues In International Arbitration, 10.08.2020, https://www.paulweiss.com/practices/litigation/international-arbitration/publications/gdpr-issues-in-international-arbitration?id=37691

https://www.vicbar.com.au/public/adr/commercial-arbitration

ICC, Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration, 1.01.2021, https://iccwbo.org/publication/note-parties-arbitral-tribunals-conduct-arbitration

Ilan D., Privacy in M&A Transactions: Personal Data Transfer and Post Closing Liabilities, 10.11.2016, https://corpgov.law.harvard.edu/2016/11/10/privacy-in-ma-transactions-personal-data-transfer-and-post-closing-liabilities/#:~:text=M%26A%20transactions%20often%20involve%20the,contractors%2C%20suppliers%20and%20business%20partners

International Council for Commercial Arbitration (ICCA), International Bar Association (IBA), The ICCA-IBA Roadmap to Data Protection in International Arbitration (Public Consultation Draft), February 2020

Lomas N., EU-US data transfers deal could be finalized by end of year, says bloc, 12.04.2022, https://techcrunch.com/2022/04/12/eu-us-data-transfers-deal-expected-timeline/

Respondek A., Lim T., The Impact Of The „General Data Protection Regulation (GDPR)" On International Arbitration Proceedings, September 2020, http://www.hk-lawyer.org/content/impact-%E2%80%9Cgeneral-data-protection-regulation-gdpr%E2%80%9D-international-arbitration-proceedings

Schrems II landmark ruling: A detailed analysis, https://www.nortonrosefulbright.com/en/knowledge/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis

The 2020 Protocol on Cybersecurity in International Arbitration, adopted by the International Council for Commercial Arbitration, the New York City Bar Association and the International Institute for Conflict Prevention and Resolution, https://www.arbitration-icca.org/cybersecurity-international-arbitration-icca-nyc-bar-cpr-working-group

The 2021 International Arbitration Survey: Adapting arbitration to a changing world, https://www.whitecase.com/sites/default/files/2021-06/qmul-international-arbitration-survey-2021-web-single-final-v2.pdf

The ICC Commission Report on Information Technology in International Arbitration, https://iccwbo.org/content/uploads/sites/3/2017/03/icc-information-technology-in-international-arbitration-icc-arbitration-adr-commission.pdf

The LCIA 2020 Annual Casework Report, https://www.lcia.org/media/download.aspx?MediaId=855

Touzet J., Gambarini C., Document Production, 24.12.2021, Jus Mundi, https://jusmundi.com/en/document/wiki/en-document-production

Vannieuwenhuyse G., The Rise of M&A Arbitration, Kluwer Arbitration Blog, 6.04.2021, http://arbitrationblog.kluwerarbitration.com/2021/04/06/the-rise-of-ma-arbitration/

Vienna International Arbitral Centre, Arbitration Privacy Policy, https://www.viac.eu/en/privacy-statement

Why international arbitration is ideally suited for the Life Sciences and Healthcare sector, 23.02.2021, https://www.osborneclarke.com/insights/international-arbitration-ideally-suited-life-sciences-health-sector

Working Party 29, Guidelines on Personal data breach notification under Regulation 2016/679, 3.10.2017, https://ec.europa.eu/newsroom/article29/items/612052

Working Party 29, Opinion 4/2007 on the concept of personal data, WP 136, 20.06.2007

Working Party 29, Working Document 1/2009 on pre-trial discovery for cross border civil litigation, 11.02.2009, WP 158, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf

Zahariev M., GDPR Issues in Commercial Arbitration and How to Mitigate Them, 7.09.2019, http://arbitrationblog.kluwerarbitration.com/2019/09/07/gdpr-issues-in-commercial-arbitration-and-how-to-mitigate-them

Zahariev M., GDPR Issues In Commercial Arbitration And How To Mitigate Them, https://arbitrationbulgaria.com/2021/06/01/gdpr-issues/

LIST OF ABBREVIATIONS

Abbreviation	Definition
AG	Advocate General
CIETAC	China International Economic and Trade Arbitration Commission
CJEU	Court of Justice of the European Union
EDPB	European Data Protection Board
EP	European Parliament
EU	European Union
HKIAC	Hong Kong International Arbitration Centre
ICC	International Chamber of Commerce
LCIA	London Court of International Arbitration
OECD	Organisation for Economic Co-operation and Development
VIAC	Vienna International Arbitral Center
WP29	Article 29 Working Party (Working Party on the Protection of Individuals with regard to the Processing of Personal Data)