CHAPTER 17

Tactical Misuse of the GDPR in Arbitration: Is It an Actual Risk?

Nika Larkimo & Katja Hoppu[*]

§17.01 INTRODUCTION

The data protection landscape has evolved significantly in recent years, particularly following the entry into force of the European Union's General Data Protection Regulation (Regulation (EU) 2016/679, the 'GDPR') in May 2018. The GDPR's broad applicability has raised significant yet unanswered questions for international arbitration practitioners. Many articles have been written on the general applicability of the GDPR to arbitration proceedings. This chapter will, however, focus on a specific question: tactical misuse of the GDPR in arbitration. The chapter explores potential scenarios involving tactical misuse of data protection regulation in different stages of arbitration proceedings, and ways that the arbitral tribunal or the opposing party and its counsel may have to prevent such misconduct or react to it.

The chapter broadly defines tactical misuse as situations where a party to an arbitration invokes the GDPR with the aim of obtaining tactical benefit in the proceedings without legitimate grounds for doing so. Most often, such situations arise when a party invokes the GDPR to avoid disclosing unfavourable documents in arbitration. This chapter will focus on the GDPR. But that is not to belittle the relevance of any other pieces of data protection legislation, particularly local regulations applicable in each party, counsel, or arbitrator's home jurisdiction.

* The views expressed in this chapter are strictly those of the authors and should not be attributed in any way to Roschier, Attorneys Ltd.

This chapter is not the first to observe the possibility of misuse of data protection regulation in arbitration.[1] However, the topic is usually bypassed by mentioning that these situations should be handled on an ad hoc, case-by-case basis. While the authors of this chapter ultimately agree with this conclusion, the chapter will explore the possibility of providing general guidelines applicable in situations that arise from a party's use of data protection-related arguments for purely tactical purposes.

The first part of the chapter will set the scene by brushing up on some of the key concepts under the GDPR and their relevance in arbitration. The section will not seek to provide a comprehensive course on the GDPR, which is better left for data protection specialists but will focus on the essential concepts that impact the assessment of when tactical misuse of the GDPR is likely to be at hand.

The second part will seek to establish stages in arbitration that are most prone to tactical misuse of the GDPR and explore how likely such conduct really is in each of those.

The third part will examine ways to prevent or react to potential tactical misuse of data protection regulation. When it comes to the prevention of misuse, the chapter will seek to offer practical solutions for arbitrators and counsel by, among others, discussing what should be included in procedural orders regarding GDPR compliance in different stages of an arbitration. Further to the preventive actions, the chapter also explores possible reactions and solutions to problems that have already occurred.

The final section of the chapter will conclude the above topics and seek to identify some best practices that may help arbitrators and counsel to address potential misuse of the GDPR.

§17.02 KEY GDPR CONCEPTS AND THEIR APPLICATION TO ARBITRATION

[A] GDPR Definitions and Principles Relevant to Arbitration

The GDPR entered into force on 25 May 2018 in all EU Member States.[2] The aim of the regulation is to harmonize data privacy laws across Europe, including the protection of

1. *See, e.g.*, Komninos Komnios, *Legal Consequences for Non-compliance With the GDPR in International Arbitration*, in Stavros Brekoulakis (ed.), Arbitration: The International Journal of Arbitration, Mediation and Dispute Management, (© Kluwer Law International; Kluwer Law International 2022, Volume 88 Issue 4) s. 2.2; Rosenthal, David, *Complying with the General Data Protection Regulation (GDPR) in International Arbitration – Practical Guidance*, in ASA Bulletin, December 2019, Topic No. 5 Dealing with other Provisions of the GDPR, 2. Solution; Emily Hay, *Chapter 7: Data protection and international arbitration: never the twain shall meet?*, in Pietro Ortolani et al. (eds), International Arbitration and Technology (© 2022 Wolters Kluwer Nederland B.V., Nijmegen; Kluwer Law International 2022) p. 131.
2. The International Council for Commercial Arbitration (ICCA) and the International Bar Association (IBA) have published a joint roadmap to data protection in international arbitration, which provides useful explanations and descriptions of data protection issues in international arbitration. The document is widely referenced in this chapter, and we invite all arbitration practitioners to familiarize themselves with its content. *See* ICCA-IBA Joint Task Force on Data Protection in International Arbitration – Roadmap to data protection in international arbitration 2022. https:/

fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between the Member States.[3]

Parties to an arbitration cannot deselect the application of the GDPR when the regulation is applicable in accordance with its material and territorial scope.[4]

The GDPR defines personal data as 'any information relating to an identified or identifiable natural person'.[5] The GDPR refers to such identified or identifiable natural persons as 'data subjects'. While legal persons are not considered data subjects under the GDPR,[6] it is important to note that any personal data disclosed in a business context is also protected by the GDPR.[7] The European Commission has provided a list of examples of what information is included in the scope of personal data under the GDPR.[8] For the purposes of an arbitration practitioner, the key is to understand that the definition of personal data under the GDPR is extremely broad.

The GDPR sets strict limitations on the processing of personal data. The regulation defines processing as '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'.[9] It follows that basically any kind of handling of personal data is covered by the GDPR's definition of processing.[10] This, combined with the broad definition of personal data, means that all arbitral activities involving data that either identifies or could identify an individual are likely to be covered by the GDPR.

The GDPR is applicable in '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

/cdn.arbitration-icca.org/s3fs-public/document/media_document/ICCA_Reports_No_7_ICCA-IBA_Joint_Task_Force_on_Data_Protection_in_International_Arbitration.pdf (accessed 4 April 2023).

3. Recital 3 of the GDPR.
4. *See, e.g.*, Komninos Komnios, *Legal Consequences for Non-compliance With the GDPR in International Arbitration*, in Stavros Brekoulakis (ed.), Arbitration: The International Journal of Arbitration, Mediation and Dispute Management, (© Kluwer Law International; Kluwer Law International 2022, Volume 88 Issue 4) p. 567.
5. The GDPR, Art. 4(1).
6. Recital 14 of the GDPR.
7. Roadmap to data protection in international arbitration (ICCA-IBA) 2022, p. 9; Kathleen Paisley, *It's All about the Data: The Impact of the EU General Data Protection Regulation on International Arbitration*, in Volume 41 Fordham International Law Journal 841 (2018), p. 863.
8. *See*, *What Is Personal Data?*, EUROPEAN COMMISSION https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en (accessed 10 March 2023).
9. The GDPR, Art. 4(2).
10. *See*, *What constitutes data processing?*, EUROPEAN COMMISSION https://commission.europa.eu/law/law-topic/data-protection/reform/what-constitutes-data-processing_en (accessed 10 March 2023). *See also Paisley's* list of activities relating to documents containing personal arbitral data, which would likely be considered data processing in the meaning of the GDPR: Kathleen Paisley, *It's All about the Data: The Impact of the EU General Data Protection Regulation on International Arbitration*, in Volume 41 Fordham International Law Journal 841 (2018) pp. 864-865.

whether the processing takes place in the Union or not.'[11] In other words, when the controller or the processor of personal data is established in the EU, the GDPR cannot be avoided by moving the processing of personal data outside the EU. The GDPR also specifically prohibits the transfer of personal data to countries outside the European Economic Area[12] unless one of the prerequisites provided in Chapter 5 of the GDPR applies.[13]

The GDPR classifies actors who process personal data into data controllers and data processors.[14] In simple terms, the processor processes personal data on behalf of the controller, whereas the controller determines the purposes and means of the processing of personal data.[15] Unlike processors, controllers process personal data on their own authority and not based on instructions given to them by another actor and decide certain key elements of processing.[16] The distinction between these two concepts matters because the prerequisites for the processing of data by a controller and a processor are different.[17] Furthermore, the controller always retains the main responsibility for the processing and is primarily responsible for compliance and demonstrating compliance with the GDPR.[18] In an arbitration context, the parties and their legal counsel, members of the arbitral tribunal, and experts and witnesses are all likely to be deemed as data controllers.[19] The GDPR also establishes a concept of joint controllership, which means that several controllers jointly determine the purposes and means of data processing, and are jointly and severally liable for any violations.[20]

11. The GDPR, Art. 3(1); Recital 22 of the GDPR. Also, the GDPR, Art. 3(2) sets out that the regulation applies in the situations specified in the article to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union. The regulation aims to ensure the protection of natural persons who are in the Union where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. *See* Recital 23 of the GDPR.
12. The GDPR, Art. 44.
13. Data transfer is allowed, e.g., where an adequate level of data protection is ensured, and where 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. Transfer of personal data can also be based on an international agreement, 'such as such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State'. Also, the data subject's explicit consent to make the data transfer enables it. *See* the GDPR, Arts 45, 46 and 48 and Roadmap to data protection in international arbitration (ICCA-IBA) 2022, p. 99.
14. *See* the GDPR, Ch. 4 on controller and processor.
15. The GDPR, Art. 4(7) and (8).
16. The GDPR, Art. 28(1) and Recital 74 of the GDPR; European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p. 3.
17. The GDPR, Ch. 4.
18. Roadmap to data protection in international arbitration (ICCA-IBA) 2022, p. 12.
19. Roadmap to data protection in international arbitration (ICCA-IBA) 2022, p. 12; Emily Hay, *Chapter 7: Data Protection and International Arbitration: Never the Twain Shall Meet?*, in Pietro Ortolani et al. (eds), International Arbitration and Technology (© 2022 Wolters Kluwer Nederland B.V., Nijmegen; Kluwer Law International 2022) pp. 104-105.
20. Article 4(7) of the GDPR. It has been argued that parties and their legal counsel as well as the members of the tribunal should be determined as 'joint controllers' in arbitration under the GDPR, Art. 26. Roadmap to data protection in international arbitration (ICCA-IBA) 2022 mentions that arbitral participants will generally be data controllers, and joint controllers under certain circumstances. Joint controllers have an obligation to determine and agree their respective responsibilities for compliance with the obligations under the GDPR in a transparent

The starting point of the GDPR is that any processing of personal data requires a legal basis.[21] The possible legal bases that may allow processing of personal data are listed in Article 6 of the GDPR. In the arbitration context, the legal basis most often relied on is legitimate interest.[22] The legitimate interest in arbitration is likely to stem from, for example, the administration of justice, ensuring that the parties' rights are respected, as well as the expeditious and fair resolution of claims under the applicable arbitration rules.[23] Legitimate interest can, however, be overridden by the interests or fundamental rights and freedoms of the data subject.[24] This means that a proportionality assessment of the data subjects' rights and freedoms should be performed even when a legitimate interest in the processing of personal data exists.[25] In other words, the interests, freedoms and rights of a data subject need to be balanced with the legitimate interests of a data processor.[26] The data subject's freely given, specific, informed and unambiguous consent for processing its personal data also constitutes a legal basis for processing.[27] However, as will be discussed in more detail in the next section, relying on data subjects' consent to process personal data in arbitration is not necessarily a workable solution.

Finally, before diving deeper into the core of this chapter, it is important to understand the basic principles for data processing that the GDPR relies on.[28] As noted by one author, the application of these principles has been subject to confusion and uncertainty among arbitration practitioners.[29]

Perhaps the most important principle in the context of tactical misuse of the GDPR is the principle of data minimization, according to which personal data should be processed only to the necessary extent. What is considered necessary is assessed in relation to the purpose of the processing of the data. Compliance with the principle also requires that the processed personal data is adequate and relevant.[30] The principles of fair, transparent, and lawful processing, as well as integrity and confidentiality, are also relevant in this context.[31] The first aims to ensure that personal data is processed

---

manner, as set out in the before mentioned article of the GDPR. *See, e.g.*, Emily Hay, *Chapter 7: Data Protection and International Arbitration: Never the Twain Shall Meet?*, in Pietro Ortolani et al. (eds), International Arbitration and Technology, (© 2022 Wolters Kluwer Nederland B.V., Nijmegen; Kluwer Law International 2022) pp. 105-106.

21. The GDPR, Art. 6.
22. The GDPR, Art. 6(1)(f). *See also* Annex 5 (Checklist: Legitimate Interest Assessment) of the Roadmap to data protection in international arbitration (ICCA-IBA) 2022.
23. Roadmap to data protection in international arbitration (ICCA-IBA) 2022, p. 89.
24. The GDPR, Art. 6(1)(f). *See also* Recital 4 of the GDPR.
25. Emily Hay, *Chapter 7: Data protection and International Arbitration: Never the Twain Shall Meet?*, in Pietro Ortolani et al. (eds), International Arbitration and Technology, (© 2022 Wolters Kluwer Nederland B.V., Nijmegen; Kluwer Law International 2022) p. 115.
26. Denis Kelleher Karen Murray, *EU Data Protection Law*, Bloomsbury Professional Ltd 2018, p. 177.
27. The GDPR, Arts 4(11) and 6(1)(f).
28. Recital 39 of the GDPR provides a summary of the most important principles for data processing.
29. Kathleen Paisley, *It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration*, in Volume 41 Fordham International Law Journal 841 (2018) pp. 846-847.
30. The GDPR, Art. 5(1)(c), Recital 39 of the GDPR.
31. The GDPR, Art. 5(1)(a) and 5(1)(f).

only in such ways that data subjects can reasonably expect and in a transparent manner. The second sets out that there should be appropriate security of the personal data in place, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.[32]

Finally, the principle of accountability requires the controller to demonstrate compliance with the GDPR.[33] Hence, it does not suffice to comply with the GDPR, but the controller must also be able to demonstrate its compliance with the GDPR to avoid responsibility for breaching the regulation. This becomes crucial in arbitration when assessing what data protection measures should be recorded and how.

[B] Application of GDPR Principles to Disclosure of Personal Data in Arbitration

As a result of digitalization and fast technological development, processing extensive volumes of personal data is inevitable in modern international arbitration.[34] Understanding when the GDPR prohibits processing of personal data is important for the parties and the arbitral tribunal who wish to avoid any breaches. It also draws the line between when the reliance on the GDPR is warranted as opposed to situations where a party is likely trying to use it to obtain tactical benefit.

However, the GDPR does not expressly state when a party can refuse to submit personal data in arbitration.[35] Assessing when the GDPR prohibits disclosure of personal data in arbitration, therefore, requires understanding its general functioning.

The GDPR is only applicable to information that contains personal data.[36] However, the fact that a document contains some personal data does not automatically mean that its use in arbitration is prohibited. Often, documents can be produced in arbitration once the parts containing personal data are anonymized or pseudonymized from the document.[37] As the definition of personal data is rather extensive, the definition of anonymized data, which cannot include any identifiers, has to be correspondingly narrow.[38] It is relevant that the data subject can no longer be

32. Roadmap to data protection in international arbitration (ICCA-IBA) 2022 provides a useful guide on general data protection principles that are relevant to arbitration, *see* section 4.1 of the article on Roadmap to data protection in international arbitration (ICCA-IBA) 2022.
33. The GDPR, Art. 5(2).
34. *See, e.g.*, Komninos Komnios, *Legal Consequences for Non-compliance With the GDPR in International Arbitration*, in Stavros Brekoulakis (ed.), Arbitration: The International Journal of Arbitration, Mediation and Dispute Management, (© Kluwer Law International; Kluwer Law International 2022, Volume 88 Issue 4) p. 566; Emily Hay, *Chapter 7: Data Protection and International Arbitration: Never the Twain Shall Meet?*, in Pietro Ortolani et al. (eds), International Arbitration and Technology (© 2022 Wolters Kluwer Nederland B.V., Nijmegen; Kluwer Law International 2022) p. 101.
35. The GDPR does not even mention the word 'arbitration'.
36. The GDPR, Art. 1(1).
37. *See* Recitals 26 and 28 of the GDPR.
38. Denis Kelleher, Karen Murray, *EU Data Protection Law*, Bloomsbury Professional Ltd 2018, p. 91.

identifiable from the anonymized data.[39] Pseudonymization of data, however, is defined in the GDPR as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.'[40] In other words, pseudonymized data is coded so that the data subject cannot be identified but in such a manner that the data can later be decoded if needed.[41] Importantly, pseudonymized data is within the scope of the GDPR, whereas anonymized data is not.[42]

As noted earlier, a party may be allowed to process personal data if there is legal basis to do so. The tricky part is, however, that legal basis should be assessed separately for each situation where personal data is processed. A legitimate interest to process data at a certain stage in arbitration does not give the controller or the processor free hands to process the data as they wish throughout the lifecycle of an arbitral proceeding.[43] As mentioned above, the key question to be asked when considering the disclosure of personal data is whether there is a legitimate interest in accordance with Article 6(1)(f) of the GDPR to do so. That legitimate interest is, however, to be balanced against the data subject's fundamental rights that can prevent the processing of personal data. The same was confirmed in the context of document production in court proceedings in the CJEU Case No. C-268/21 *Norra Stockholm Bygg AB v. Per Nycander AB*.[44] The CJEU emphasized the parties' right to effective judicial protection when assessing what kind of evidence the parties are allowed to submit in dispute proceedings based on the GDPR.[45] Furthermore, the ruling clarifies that Articles 5 and 6 of the GDPR:

> must be interpreted as meaning that, when assessing whether the production of a document containing personal data must be ordered, the national court is required to have regard to the interests of the data subjects concerned and to balance them according to the circumstances of each case, the type of proceeding at issue and

39. Denis Kelleher, Karen Murray, *EU Data Protection Law,* Bloomsbury Professional Ltd 2018, p. 93.
40. Article 4(5) of the GDPR. According to Recital 28 of the GDPR, pseudonymization of personal data can help the data processors and controllers to meet their data protection obligations.
41. Kathleen Paisley, *It's All about the Data: The Impact of the EU General Data Protection Regulation on International Arbitration*, in Volume 41 Fordham International Law Journal 841 (2018), p. 903. European Union Agency for Cybersecurity has published multiple guidelines for data pseudonymization. *See, e.g.*, ENISA Pseudonymization techniques and best practices, November 2019, and ENISA Data Pseudonymization: Advanced Techniques and Use Cases, January 2021.
42. Case No. C-268/21, *Norra Stockholm Bygg AB v. Per Nycander AB*, 2 March 2023, para. 57.
43. Emily Hay, *Chapter 7: Data protection and International Arbitration: Never the Twain Shall Meet?*, in Pietro Ortolani et al. (eds), International Arbitration and Technology (© 2022 Wolters Kluwer Nederland B.V., Nijmegen; Kluwer Law International 2022) p. 117.
44. In the mentioned case, the concerned personal data was originally collected and processed for tax purposes.
45. Case No. C-268/21, *Norra Stockholm Bygg AB v. Per Nycander AB,* 2 March 2023, para. 53.

> duly taking into account the requirements arising from the principle of proportionality as well as, in particular, those resulting from the principle of data minimisation referred to in Article 5(1)(c) of that regulation.[46]

The starting point of the GDPR is that personal data can be processed only for the purpose for which the data has been collected.[47] It follows that, in principle, any data that is collected for a purpose other than arbitration should not be disclosed in the arbitration. Typically, the evidence processed by the parties and the personal data contained therein have not been created for the purposes of an arbitration.[48] Personal data is also often processed by arbitral participants who did not initially collect the personal data. In such cases, the possibility of processing the data for the purposes of arbitration should either be included in the original notice provided to the data subject or, alternatively, be compatible with the purposes of processing that have been identified in such notice.[49]

When assessing whether disclosure of personal data is allowed in arbitration, it is also worth keeping in mind that the disclosure of personal data should be relevant. The principle of data minimization in Article 5(1)(c) provides that unnecessary processing of personal data should be avoided.[50] Of course, in an arbitration context, information that is relevant for one party may not be equally important for the other. Especially in the context of document production, parties are often obliged to produce documents that are not relevant to making their points but rather the opposite. An objective assessment of the application of the data minimization principle accordingly seems warranted. It is also often hard to tell in advance what pieces of data become relevant in arbitration. Thus, assessing the scope of and ensuring compliance with the principle of data minimization is not a simple task.

Finally, as mentioned earlier, disclosure of personal data is allowed when the data subject has given its consent for the processing of its personal data. While arguably the clearest of the legal bases provided under Article 6 of the GDPR, the data subject's consent as a basis to process personal data in arbitration can be somewhat problematic to rely on. Issues may arise if the data subject withdraws its consent for the processing of its data at any stage of the arbitration.[51] It is included in the nature of valid consent that the data subjects must have an actual opportunity to withdraw their

46. Case No. C-268/21, *Norra Stockholm Bygg AB v. Per Nycander AB*, 2 March 2023, para. 59.
47. The GDPR, Art. 6(3) and 6(4).
48. Roadmap to data protection in international arbitration (ICCA-IBA) 2022, p. 24.
49. Roadmap to data protection in international arbitration (ICCA-IBA) 2022, p. 24. The points mentioned in this paragraph are included in the regulation of the GDPR mainly throughout the 'purpose limitation' that is set out in Art. 5(1)(b) of the GDPR.
50. *See also* Recital 39 of the GDPR.
51. Rosenthal, David, *Complying with the General Data Protection Regulation (GDPR) in International Arbitration – Practical Guidance*, in ASA Bulletin, December 2019, Topic No. 4 How Personal Data may be processed, 2. Solution; Emily Hay, *Chapter 7: Data Protection and International Arbitration: Never the Twain Shall Meet?*, in Pietro Ortolani et al. (eds), International Arbitration and Technology (© 2022 Wolters Kluwer Nederland B.V., Nijmegen; Kluwer Law International 2022) p. 114.

permission without suffering any penalty if they change their mind.[52] Also, it has been argued that consent is unlikely to be a sufficient basis for the processing of large volumes of documents containing personal data, which is commonplace in arbitration.[53] Finally, obtaining each data subject's separate consent is often impracticable in arbitration, which may comprise thousands of documents containing hundreds of data subjects' personal data. It follows that in arbitration, reliance on other legal bases for the processing of personal data is recommended, if possible, over the data subject's consent.[54]

§17.03 STAGES OF ARBITRATION PRONE TO TACTICAL MISUSE OF THE GDPR

A party to an arbitration has the right and the obligation to invoke the GDPR when processing of personal data is not allowed. A party may, however, also try to invoke the GDPR to gain tactical benefit, without having an actual obligation to do so.

It is fair to assume that in arbitration, most of the personal data is contained in evidence. It is widely accepted that the likelihood of a party invoking the GDPR increases in connection with the taking of evidence, especially in document production.[55]

A party may invoke the GDPR to object to a request for document production or to refuse to comply with an order to produce documents. As outlined in the previous section, in such scenarios, it is key to understand what the actual scope of the GDPR is and how it limits a party's possibility to disclose personal data.

In many instances, redacting personal data from the documents to be disclosed is required to fully comply with the GDPR. A question arises: when does the production become 'unreasonably burdensome' in the meaning of Article 9.2(c) of the IBA Rules, constituting a valid ground to object to a document production request? Unreasonable burden can take many forms, and it has been left to the arbitral tribunal's discretion to determine what kind of burden is considered unreasonable.[56] Eventually, it is for the arbitral tribunal to determine whether a party's objection on the ground of unreasonable burden based on the GDPR has a legitimate basis.

The scope of any redactions is also prone to create issues in arbitration. Parties' attempting to redact information unfavourable to their case on the basis of legal

52. *See* Working Document on a Common Interpretation of Art. 26(1) of Directive 95/46/EC of 24 October 1995 (Art. 29 Data Protection Working Party, 2093/05/EN WP 114, 2005), p. 11.
53. Kathleen Paisley, *It's All about the Data: The Impact of the EU General Data Protection Regulation on International Arbitration*, in Volume 41 Fordham International Law Journal 841 (2018), p. 887.
54. *See, e.g.*, Roadmap to data protection in international arbitration (ICCA-IBA) 2022, p. 43.
55. It has been stated that issues of data protection can arise in particular in document production. *See* 'Chapter 20: Data Protection and Cybersecurity', in Neil Kaplan, Chiann Bao, *So, Now You Are an Arbitrator: The Arbitrator's Toolkit* (© Kluwer Law International; Kluwer Law International 2022), p. 152.
56. The IBA Commentary on the Revised Text of the 2020 IBA Rules on the Taking of Evidence in International Arbitration (2020), p. 29.

privilege or commercial confidentiality is not uncommon in international arbitration. Similar objections can be made based on the GDPR.

An added complexity is that parties seldom refer to the GDPR as the only basis to object to a document production request but instead combine it with other reasons, such as privilege and commercial confidentiality.[57] To address concerns of confidentiality and trade secrets, parties may request that certain evidentiary documents be displayed only to the arbitral tribunal and legal counsel representing the parties. This may help resolve situations where there are reasons to believe that a party has invoked commercial confidentiality without having an actual basis to do so. The same is, however, unlikely to help in the context of a party invoking the GDPR. When the GDPR prohibits the disclosure of personal data, it is not possible to bypass such prohibition by disclosing the data to a smaller group.

Another part of taking evidence where the GDPR could be invoked is witness examination. Technically, a witness could try to refer to the GDPR to avoid having to answer a difficult question. However, this does not seem very likely, and we have not heard of such instances. It would require courage from a witness to do so. For a witness to invoke the GDPR also carries the risk of ultimately damaging the witness' credibility, as it may be perceived as a way to avoid having to answer difficult questions.

Another relevant aspect of compliance with the GDPR is its potential role in the recognition and enforcement of arbitral awards. The CJEU has ruled that arbitrators must apply the provisions of the EU law falling under the EU public policy.[58] Member State courts are obliged to verify the compliance of an arbitral award with mandatory EU law on their own motion.[59] The Advocate General in the ECJ Case No. C-681/13 aptly set out in his opinion that 'although every Member State is to determine the requirements of its own public policy, there is still within national public policy a core set of values, principles and fundamental rules of the European Union, with the same legislative content, that every Member State must take into account.'[60] A party could seek to set aside an award on the basis of a violation of public policy if it has reasons to believe that the GDPR has not been complied with in the proceedings and the award is contrary to the regulation of the GDPR.[61]

Whether breaches of the GDPR affect the validity of an arbitral award is a complex issue. GDPR breaches often concern persons who are not involved in the

57. *See, e.g.*, the IBA Rules on the Taking of Evidence in International Arbitration, Art. 9.2(b) and 9.2(e).
58. Case No. C-126/97, *Eco Swiss China Time Ltd. v. Benetton International NV*, CJEU, 1 June 1999, para. 37.
59. *See, e.g.*, Komninos Komnios, *Legal Consequences for Non-compliance with the GDPR in International Arbitration*, in Stavros Brekoulakis (ed.), Arbitration: The International Journal of Arbitration, Mediation and Dispute Management (© Kluwer Law International; Kluwer Law International 2022, Volume 88 Issue 4) p. 572.
60. Opinion of Advocate General Szpunar delivered on 3 March 2015. *Diageo Brands BV v. Simiramida*-04 EOOD, section 39.
61. Komninos Komnios, *Legal Consequences for Non-compliance with the GDPR in International Arbitration*, in Stavros Brekoulakis (ed.), Arbitration: The International Journal of Arbitration, Mediation and Dispute Management, (© Kluwer Law International; Kluwer Law International 2022, Volume 88 Issue 4) p. 578.

arbitration.[62] Setting aside an arbitral award that the data subject whom the breach concerns does not even have access to seems unlikely. However, interestingly, for the topic of this chapter, it has been suggested that a party to an arbitration could knowingly violate or have the arbitral tribunal violate the provisions of the GDPR to have the option to dispute the validity of the award after it has been rendered.[63] While the possibility for a party to rely on its own breach to have an arbitral award set aside sounds somewhat far-fetched, this cannot be excluded. This again highlights the importance for the arbitral tribunal to understand the applicable data protection regulations, which is likely to be the best protection against their misuse.

§17.04 PREVENTING AND REACTING TO TACTICAL MISUSE OF THE GDPR

[A] Data Protection Framework Provided in Institutional and Other Rules

The natural first place for arbitrators and parties to seek guidance when assessing procedural issues is the applicable institutional rules.

Arbitration institutes have taken different approaches to addressing data protection issues. To date, most institutional rules are completely silent on data protection. For example, the ICC (2021), HKIAC (2018), FAI (2020) and SCC (2023) rules do not even mention data protection. The ICC Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration (2021), however, emphasizes the importance of data protection in international arbitration and establishes key principles to be followed when processing personal data under the GDPR. The Note further highlights that the parties and their representatives, as well as the arbitral tribunal, are obliged to ensure a reasonable level of data security in the arbitration.[64] The ICC has also provided a model for the data protection clause to be used in Procedural Order No. 1.[65]

Of the institutional rules reviewed for the preparation of this chapter, the only rules to expressly oblige the arbitral tribunal to consider data protection issues were the LCIA (2020) and the ICDR Rules. The ICDR Rules contain a recommendation to the

62. Komninos Komnios, *Legal Consequences for Non-compliance with the GDPR in International Arbitration*, in Stavros Brekoulakis (ed.), Arbitration: The International Journal of Arbitration, Mediation and Dispute Management, (© Kluwer Law International; Kluwer Law International 2022, Volume 88 Issue 4) p. 574.
63. Komninos Komnios, *Legal Consequences for Non-compliance with the GDPR in International Arbitration*, in Stavros Brekoulakis (ed.), Arbitration: The International Journal of Arbitration, Mediation and Dispute Management, (© Kluwer Law International; Kluwer Law International 2022, Volume 88 Issue 4) p. 574.
64. The ICC Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration (2021), section E – Protection of Personal Data.
65. *See* ICC Model Data Protection Clause for Procedural Order 1, which is intended for arbitrators, to provide guidance in the drafting of data protection clause in Procedural Order one, where issues related to the GDPR are addressed, https://cdn.iccwbo.org/content/uploads/sites/3/2021/01/icc-model-po1-data-protection-english.pdf (accessed 4 April 2023).

arbitral tribunal to discuss data protection to provide for an appropriate level of security and compliance.[66]

Article 30A of the LCIA rules clarifies that '[a]ny processing of personal data by the LCIA is subject to applicable data protection legislation' and refers to the LCIA's data protection notice. The provision also requires the arbitral tribunal to, 'at an early stage of the arbitration', consult the parties as to the need of adopting 'any means to address the processing of personal data produced or exchanged in the arbitration in light of applicable data protection or equivalent legislation'. The LCIA or the arbitral tribunal may also issue binding directions to the parties addressing data protection.

The IBA rules on the Taking of Evidence in International Arbitration (2020) mention data protection issues. But they do not provide much guidance: the IBA Rules simply highlight that it is advised to consider 'treatment of any issues of cybersecurity and data protection' as part of the evidentiary issues.[67]

As such, it is fair to conclude that institutional rules and guidelines do not provide many tools for arbitrators or counsel to address the possibility of misuse of the GDPR. Accordingly, such tools need to be sought from other sources.

[B] Tools for Preventing Tactical Misuse of the GDPR

In the authors' view, the first step in preventing tactical misuse of GDPR in arbitration is making sure that all participants in an arbitration understand the basics of the GDPR and its implications. By way of a simple demonstration, it is harder for a party to argue that an entire, large category of documents cannot be disclosed due to the GDPR if the arbitral tribunal and the opposing side understand that the GDPR only prevents disclosure of personal data.

The second step is to document such understanding. As suggested in the ICCA-IBA Roadmap to data protection in international arbitration, a natural place for such documentation is Procedural Order No. 1 or a separate Data Protection Protocol.[68] Addressing the GDPR in a procedural order signals to the parties that the arbitrators are familiar with the GDPR and take its implications seriously.

The previous step raises an obvious question: what should be documented? The ICCA-IBA Roadmap to data protection in international arbitration lists eight data protection issues that should be recorded. The listed issues include, for instance, the legal basis for processing and data transfer, disclosure or production of documents, data security and data breach protocols.[69] In addition to the listed issues, the tribunal should clarify in Procedural Order No. 1 that it can draw adverse inferences from a

66. ICDR International Dispute Resolution Procedures Rules, Amended and Effective 1 March 2021, Art. 22(3) of the International Arbitration Rules.
67. The mention of data protection was added in the revised text of the 2020 rules. The IBA Commentary on the Revised Text of the 2020 IBA Rules on the Taking of Evidence in International Arbitration (2020), p. 6.
68. Roadmap to data protection in international arbitration (ICCA-IBA) 2022, p. 41. The Roadmap collectively refers to data protection rules set out in a procedural order, terms of reference or data protection protocol as 'Data Protection Directions'.
69. Roadmap to data protection in international arbitration (ICCA-IBA) 2022, p. 42.

party's failure to produce documents. The ICCA-IBA Roadmap provides sample language for inclusion in a procedural order where the rules of the GDPR are to be followed.[70]

As mentioned above in section 3, the likelihood of a party invoking the GDPR increases in connection with the taking of evidence, and especially document production. The ICCA-IBA Roadmap lists issues related thereto that should be addressed in a procedural order to avoid them being raised later on in the proceedings. Such issues include the following:

> (1) limiting disclosure/data minimisation (taking into account the IBA Rules where applicable); (2) redaction/pseudonymisation in light of the applicable data protection standard; (3) entering into confidentiality provisions/protective orders; and (4) entering into standard contractual clauses or another adequate safeguard for third-country data transfers so that additional safeguards are not required, or where that is not feasible, employing a derogation when possible.[71]

As noted in the ICCA-IBA Roadmap, addressing these issues at the beginning of the proceedings saves money and time.[72] It is fair to assume that the parties are more consensual when agreeing on the common ground rules in the procedural order than when facing actual problems in the arbitration. One should also keep in mind that the parties to an international arbitration sometimes need to comply with data protection regimes that differ from each other. Agreeing on related issues helps to ensure compliance with all applicable data protection laws in the arbitration.[73]

At the end of the day, the arbitral tribunal will need to decide on applying data protection measures on a case-by-case basis. Applying such measures will depend on many circumstances, for example, the type of processing being undertaken, the type of data, including the assessment of the damages that the disclosure may cause, and the security measures of the arbitral participants.[74]

While procedural orders are ultimately issued by arbitral tribunals, making sure that those address data protection issues is not only in the arbitral tribunal's interest. Counsel also have an interest in, and arguably bear a responsibility for, ensuring that the tribunal is oriented in making the arbitration as GDPR-compliant as possible. Thus, counsel should review the draft procedural order carefully with respect to data protection issues, propose necessary additions and flag any potential issues they find. In case data protection is not addressed by the arbitrators, it is for the parties' counsel to suggest that the required language be included. In case the parties disagree on data protection measures that should be implemented in the arbitration, it is highly recommended that the tribunal provides the parties with an opportunity to address

70. Roadmap to data protection in international arbitration (ICCA-IBA) 2022, p. 42, and Annex 7.
71. Roadmap to data protection in international arbitration (ICCA-IBA) 2022, p. 48.
72. Roadmap to data protection in international arbitration (ICCA-IBA) 2022, p. 48.
73. Emily Hay, *Chapter 7: Data Protection and International Arbitration: Never the Twain Shall Meet?*, in Pietro Ortolani et al. (eds), International Arbitration and Technology, (© 2022 Wolters Kluwer Nederland B.V., Nijmegen; Kluwer Law International 2022) p. 112.
74. Roadmap to data protection in international arbitration (ICCA-IBA) 2022, p. 50.

what measures they consider reasonable and proportionate in the arbitration before issuing a procedural order on such measures.[75]

While addressing data protection issues early on in the proceedings is perhaps likely to limit the possibilities of misuse of the GDPR or other data protection regulations, it will not entirely prevent such misuse. It is, therefore, worthwhile considering how a party or an arbitrator should react to any misuse of the regulation.

[C] Possible Reactions to Tactical Misuse of the GDPR in Arbitration

Sometimes, the arbitral tribunal or a party may have reasons to believe that the other party is hiding behind the GDPR without a legitimate reason. As noted earlier, the parties are most likely to wrongly invoke the GDPR in connection with document production. A party may object to a document production request or refuse to comply with a tribunal's document production order.

The opposing party has limited ways to act on its own in such situations and will often need to escalate its concerns to the arbitral tribunal. In many instances, the party that has requested the documents has a better understanding of the likely content of the documents being withheld than the arbitral tribunal, which may help that party to demonstrate why the GDPR is unlikely to apply. In such scenarios, it is in the party's interest to try to clarify why it is unlikely that the GDPR impacts the other party's possibility to disclose information.

From an arbitral tribunal's perspective, the most obvious tool in its toolbox when detecting possible improper reliance on the GDPR is to request a detailed reasoning for the withholding of information. At a minimum, the party should be able to indicate which articles and sections of the GDPR prevent the disclosure of information. The party's reasoning is likely to reveal whether there are valid grounds to withhold the information based on the GDPR or not.

Refusing to submit a whole document due to data protection restrictions is very rarely, if ever, justified.[76] Such behaviour should usually raise red flags. While most GDPR concerns can typically be dealt with by redactions, the necessity and scope of such redactions may also result in debate.

When it comes to assessing the scope of redactions, the arbitral tribunal is again typically relying on the reasoning of the redacting party. If the other party successfully challenges that reasoning or it otherwise fails to convince, the arbitral tribunal should have the power to ask the redacting party to revisit its redactions and resubmit the documents with fewer redactions.

Finally, if the methods above have proved inefficient, but the arbitral tribunal still has its suspicions over the redactions or refusal to produce documents, a reminder to the parties of the possibility of drawing adverse inferences might help.[77] As in similar situations, this is often considered as the last warning by the arbitral tribunal,

75. *See, e.g.*, American Arbitration Association, International Centre for Dispute Resolution, Best Practices Guide for Maintaining Cybersecurity and Privacy, p. 3.
76. Roadmap to data protection in international arbitration (ICCA-IBA) 2022, p. 50.
77. *See*, *e.g.*, the IBA Rules on the Taking of Evidence in International Arbitration, Art. 9(6) and 9(7).

signalling that it is not convinced, but any undesirable consequences can still be avoided. Even after such a reminder, the arbitral tribunal can still consider whether drawing adverse inferences in the situation at hand exists.

§17.05 CONCLUSIONS

The arbitral tribunal is put in a difficult position when having to decide whether a party has a legitimate basis to rely on the GDPR or not. On the one hand, the arbitral tribunal should not allow a party to use the GDPR to obtain tactical benefit by taking every GDPR-related argument at face value. On the other, the potential consequences of a GDPR breach could be serious[78] and even put the validity of the arbitral award at risk.

While the GDPR raises difficult questions, playing ostrich is certainly not the answer. Instead, the best way to prevent and react to potential misuse of the GDPR is to understand the basics of the GDPR. At the end of the day, while the material and territorial applicability of the GDPR is broad, there are only so many instances where a party can effectively invoke the GDPR in arbitration. Understanding the key principles and legal basis required for processing of personal data under the GDPR is often sufficient for assessing if a party has grounds to invoke it or if it is more likely that such invoking has been done to obtain tactical benefit. Arbitral tribunals have wide powers to probe further information on the grounds on which a party is relying on the GDPR and are encouraged to do so.

Finally, addressing data protection issues early on in any arbitral proceedings is key not only to ensure compliance but is also likely to reduce a party's willingness and possibilities to rely on data protection regulation later without an actual basis to do so.

78. Under Art. 83(5) of the GDPR, an infringement of a data subject's rights is subject to administrative fines of up to EUR 20,000,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. Non-compliance with the GDPR may also result in civil liability of the data controller or processor. *See, e.g.*, Komninos Komnios, *Legal Consequences for Non-compliance with the GDPR in International Arbitration*, in Stavros Brekoulakis (ed.), Arbitration: The International Journal of Arbitration, Mediation and Dispute Management (© Kluwer Law International; Kluwer Law International 2022, Volume 88 Issue 4) p. 567.