GDPR Issues in Commercial Arbitration and How to Mitigate Them

Kluwer Arbitration Blog
September 7, 2019

Martin Zahariev (Dimitrov, Petrov & Co.)

Please refer to this post as: Martin Zahariev, 'GDPR Issues in Commercial Arbitration and How to Mitigate Them', Kluwer Arbitration Blog, September 7 2019, http://arbitrationblog.kluwerarbitration.com/2019/09/07/gdpr-issues-in-commercial-arbitration-and-how-to-mitigate-them/

The new EU data protection framework, in particular the General Data Protection Regulation (GDPR) applicable as of May 2018, dramatically shifted the focus of all organizations towards ensuring transparency and accountability in their data processing operations. The broad material scope of GDPR practically affects any private organization and practitioner within the EU. Moreover, in certain cases its territorial scope may extend outside the EU, thus turning non-EU economic operators (especially those monitoring/ targeting natural persons in EU with goods/services) into possible addressee of its rules. GDPR's sanctions reach EUR 20 million or 4% of the worldwide annual turnover of the preceding financial year (whichever higher). Multimillion fines have already been imposed in multiple jurisdictions such as France (see the fine imposed on Google here), UK (see the fine intention of UK supervisor to fine British Airways and Marriott International here and here), Bulgaria (see the fine imposed on the National Revenue Agency and DSK Bank EAD here and here). In light of the above, GDPR has established itself as a factor to be taken seriously.

Commercial arbitration is no exception, as GDPR applies to the activities of courts and other judicial authorities (recital 20), as well as to the activities of lawyers (recital 91). This means that any data processing within the dispute resolution process, either before court or under ADR mechanisms, including arbitration, must be performed in accordance with the GDPR requirements.

Who is Who in Arbitration from GDPR Perspective?

In order to precisely identify the roles and the related responsibilities of the key players in arbitration, one must carefully apply the GDPR rules to the underlying legal framework governing commercial arbitration. In general, there are very strong arguments allowing for the arbitral 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, *i.e*. as those who determine the purposes and means of personal data processing.

The arbitrator's role is more complex and could, to some extent, depend on the national peculiarities regulating the arbitrator's relations with the arbitral institution and the concerned parties. The institutions, however, provide administrative support for resolving disputes, rather than resolving the disputes themselves. From that perspective, the consideration and the final resolution of a dispute, as well as the related data processing, turn arbitrators (similarly to lawyers) into data controllers. These conclusions trigger numerous data governance obligations under GDPR, including but not limited to:

- informing the concerned data subjects about the processing (via documents such as privacy notices and privacy policies – Art. 12-14 of GDPR);
- being able to handle requests for exercising the data subjects' rights (Art. 15-22 of GDPR);
- regulating in an appropriate manner the relations with processors they might use (*e.g.* cloud service providers, translators, accountants, etc. – Art. 28 of GDPR);
- keeping records of processing activities (Art. 30 of GDPR);
- implementing appropriate measures for ensuring security of the personal data processed (Art. 32 of GDPR), etc.

Whether arbitrators being part of the same tribunal are joint controllers under the meaning of Art. 26 of GDPR is an even more complex question. 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. In addition, arbitrators are usually subject to different regulations (*e.g.* compliance, tax, accounting regulations, etc.). Therefore, 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.

The accountability principle, *i.e.* being able at any time to prove that you are GDPR compliant, however, remains at stake. Therefore, as a matter of good practice (although not explicitly required for 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. 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. The agreement should at minimum regulate aspects such as:

- what personal data will be collected and otherwise processed;
- what types of 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;
- what the main responsibilities of the arbitrators and institutions as independent controllers will be.

To Consent or Not to Consent?

The cliché in arbitration reads that "consent is the cornerstone of arbitration". As consent is one of the grounds for processing of personal data and probably the most popular one, a reasonable question arises – whether arbitral institutions and arbitrators should try to obtain consent from the parties involved in arbitration for the processing of the related personal data.

Although from civil law perspective the consent is necessary in order to enter into the arbitration agreement, consent as legal ground for data processing under GDPR is *not* appropriate in arbitration proceedings. The consent could be withdrawn freely and just as easily given at any time. This allows the parties to abuse the fair process by withdrawing (1) their consent for the processing – if the party is a natural person, or (2) the consent of their managers, employees and counsels – if the party is a legal entity, which will require an immediate termination of the data processing. Having the possibility to unilaterally influence the normal course of the proceedings would undoubtedly result in an undesired outcome.

GDPR offers far more solid alternatives for data processing within legal disputes, where consent for data processing should *not* be requested from the parties and their representatives, such as:

- the legitimate interest (Art. 6(1)(f));
- the necessity to perform a contract where one of the parties to the dispute is a natural person (Art. 6(1)(b), since arbitration is of contractual nature and actually constitutes provision of ADR service); and
- in certain cases – legal obligation (Art. 6(1)(c), especially where certain documents containing personal data must be retained for tax, accounting or accountability purposes).

The legitimate interest could also serve as a legal ground for providing the ADR services in B2B arbitrations.

Independence of the Judiciary vs. Accountability and Control

Last but not least, GDPR provides for administrative control by a supervisory authority, which might raise concerns among the legal community, especially in the context of ensuring the independence of the judiciary. If a court, arbitral tribunal or arbitrator could be audited and eventually fined by administrative body which is not part of the judiciary, this could be considered as a tool for unlawful influence in the dispute resolution activity of these bodies and individuals. GDPR takes this risk into account and seeks to mitigate it by explicitly regulating the possibility to entrust supervision of data processing operations related to the performance of the judicial tasks, including decision-making, to specific bodies within the judicial system of the Member States, which should, in particular ensure compliance with the rules of GDPR (recital 20).

In Bulgaria these tasks are entrusted to the Inspectorate with the Supreme Judicial Council (SJC). SJC is a specially designated body responsible for the recruitment, promotion, demotion, relocation and dismissal of judges and prosecutors. The Inspectorate is an independent body within SJC exercising control over the activities performed in the judiciary, and with the latest amendments to the data protection legislation – over data processing activities as well. Although the Bulgarian legislation regulates only the supervision of data processing activities of the state courts by the Inspectorate, it appears more than reasonable to conclude that the data processing activities of arbitral institutions and arbitrators should be supervised by the Inspectorate as well. Dispute resolution via arbitration should, in a broad sense, also be deemed part of the judiciary and ensuring its independence is equally important.

GDPR and its correlation with commercial arbitration is a very complex matter. A thorough analysis of these issues can be found in the monograph *Data Protection in Commercial Arbitration: In the Light of GDPR* published earlier this year. The book addresses the most important data protection issues in commercial arbitration, from the roles and responsibilities of the key players in arbitration, such as arbitrators, institutions, appointing authorities, etc. to some really sophisticated problems like usage of AI for the purposes of ADR. The book also contains a sample GDPR privacy policy for arbitral institutions which can be used in practice with minor modifications.

The table of content, the academic reviews and the foreword to the book can be found here – M. Zahariev, Data Protection in Commercial Arbitration_In the Light of GDPR.

The views and opinions expressed herein are those of the author and do not necessarily reflect those of Dimitrov. Petrov & Co., its affiliates, or its employees.