DOI: 10.52028/rbadr.v3i5.9

EU Data Protection Regulation and How It Affects Arbitration and ADR-ODR

Olga N. Tsiptse

Lawyer at Supreme Court of Greece. Accredited Mediator of Ministry of Justice & Arbitrator at Court of First Instance in Greece. DPO – GDPR expert. In German School of Thessaloniki Greece etc.

Abstract: On May 2018 a European Regulation, with direct force to all European Members, was in action. The General Data Protection Regulation, EU2016/679. A severe Regulation that was published in 2016 and set a 2-year period of time for all the Member States to be adjusted. This text, that implies huge fines for noncompliance, also affects the ADR mechanisms, like Arbitration, Mediation, etc. There is a paramount importance Principle of accountability, that GDPR implies, which requires data controllers to take personal responsibility for data protection compliance and record the measures they take to comply with their data protection obligations. Even almost 3 years have passed, the issues still remain: How is the interaction between ADR and GDPR? Which are the roles of the actors of alternative dispute resolution methods, and due to these roles which are the responsibilities? What is considered a lawful process, in accordance with GDPR, during the procedure of an ADR mechanism? It is also paramount to take into consideration, that the scope of that European Regulation affects directly even actors of non-EU territory, according to article 3.2 & 3 GDPR: 2. *This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: - 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 – the monitoring of their behavior as far as their behavior takes place within the Union. 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.*

Keywords: GDPR & Data Protection. ADR Mechanisms. Mediation. Arbitration. European Members. Human Rights. Proportionality Test. Legal Basis.

Introduction

All human beings have three lives:
public, private, and secret.

Gabriel García Márquez

Protection of personal data[1] is absolutely a human right, but it is not an absolute human right. Data protection is considered as high priority for, at least, European Nations and that is the reason, for the increasing concerns about how retaining personal data protection against specific needs, *e. g.* through out-of-Court procedures or the recently need for e-justice and e-out of court procedures, that might be dominant especially in pandemic SARS-CoV-2 (hereafter COVID-19 or coronavirus) era and of course after this period. Despite these concerns, data protection, through these tough years, is not taken for granted. The changes of the data process worldwide, are radical, also the speed of these changes is vertiginous and the humanity was not ready for such eventuality.

Referring to a human right as a non-absolute right, indicates, and therefore highlights, the difficulties in its protection. The difficulties protecting personal data tends to peak in emergencies and force majeure situations, when other individual rights such as public health and safety, and in general public interest, must be protected as well. When these emergencies are faced, and while considering personal data protection not being an absolute human right, it shall be balanced in and for every separate case that arises. There is no general rule. The duty of balancing this top priority right[2] with others, shall be "in accordance with the Principle of Proportionality", a cornerstone Principle that is diffused in the legislation of Regulation (EU) 2016/679 of European Parliament and Council of 27th April 2016[3] (hereafter the Regulation or GDPR), it is also mentioned in all relevant legislation, guidelines, opinions, statements etc.[4]

At this point, a separation of concepts must be realized. Protection of personal data is only an area of the broader concept of privacy. In fact, data protection

[1] See the relevant definitions in Article 4 of the Regulation (EU) 2016/679, in force since 25th May, 2018, and especially: "Article 4(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); 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; (2) 'processing' 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; (…) etc."

[2] Quite contradictory, on the writer's opinion, because this priority is finally on the surface and not substantial.

[3] GDPR Recital 4: "The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognized in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."

[4] Article 9A Constitution of Greece, Guidelines and opinions of EDPB (European Data Protection Board) and national DPA's (Data Protection Authorities) that are going to be analyzed below.

right serves more purposes than privacy, and in that sense it is broader than privacy. On the other hand though, privacy is broader than data protection, because it is consisted by other elements, as the right to be alone, the right to respect private or family life.[5] Consequently, the above two concepts, data protection and privacy, are not the same but still both are connected and interacting. The data protection right depends on privacy and, at a certain level, it secures privacy. It is not only protected when it is violated, but it obligates all the processors to be organized to a certain regulatory field. And that leads to a conclusion, that though it is a non-absolute right – and therefore it shall be balanced with other rights, in order the legal purposes of data processing to be indicated against the legitimate intrusion of that right – data protection seems to be a "constitutionalized" right, that is volatile depending on the purposes that is needed to protect.

Another topic, that shall be examined, is the *lawful processing of data*, especially of the special categories of personal data. Lawful processing is one of the principles,[6] that are relating to process of any category of data. The GDPR repeats the implication of the previous Directive 95/46,[7] and imposes the lawful processing of personal data. This principle is not defined exactly in the provisions, but it is implied in recital 40 GDPR, where a reference to lawful processing of data is also made.[8] More specifically, entities shall not process data, and mostly special categories of data, unless there is a legal basis for that action, a legitimate ground.[9] And to that point, the above prohibition must be seen as an exception.[10] This exception, that also consists one of the principles in protecting data, leads to the reduction of personal data protection. Data protection limitation is also recognized in Article 52,(1) of the European Charter of Human Rights (ECHR).[11] Therefore, in case of conflicting rights, some are limited and some prevail.

[5] Article 8 ECHR (European Charter for Human Rights).

[6] Other principles are the processing of personal data shall be Fair, Transparent, Limited in purpose, in storage and in quantity, Accurate, and finally Confidential.

[7] Article 6(1)(a) GDPR.

[8] RÜCKER; KUGLER, 2018, p. 50-51.

[9] Legitimate grounds for processing data are restrictively referred to Article 6 GDPR, and for special categories of data, to Article 9 GDPR. Also are referred to national laws following GDPR.

[10] "The right to personal data protection is not an absolute right; it may be limited if necessary for an objective of general interest or to protect the rights and freedoms of others" (See, for example, Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert *v.* Land Hessen [GC], 9 November 2010, para. 48) (CJEU, 2018, p. 35).

[11] "As long as those limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others."

ADR and GDPR

The above mentioned made all organizations, European and non-European,[12] to focus towards ensuring transparency and accountability in their data processing operations. GDPR's territorial scope may extend outside the EU, thus turning non-EU economic operators, mostly when there is monitoring natural persons in EU with goods and services. The sanctions Regulation threatens, upon noncompliance reach EUR 20 million or 4% of the worldwide annual turnover of the preceding financial year (whichever higher). Multimillion fines have already been imposed towards many organizations and entities.

It is unavoidable that court procedures[13] and ADR as well, as Arbitration, Mediation etc. would be affected, either by this European Regulation or other Bills/ Acts have already been regulated globally. In other words, any court procedure or ADR method shall be in accordance and in compliance to and with GDPR requirements, in compliance to and with all the Guidelines European Data Protection Board (EDPB) and finally, to and with national Authorities issues or have already issued.

Roles and Responsibilities

When starting the application and the compliance with GDPR, of paramount importance is the awareness of the role and responsibilities the actors play and have, *e. g.* in Arbitration. Arbitration is divided into ad hoc and Institutional. In the first occasion, the distinction of roles is rather easy. The case becomes complicated when many persons are involved in the data flow and have access to many data, and that case is Institutional Arbitration.

According to the European Regulation, we can consider the Arbitration Institutions as data controllers, because due to the legal text the key point is, that they determine the purposes and means of personal data processing. More complexity is faced, regarding the Arbitrator, sole or Tribunal. Arbitrator is independent player and not the Institution as such. So, what role has Arbitrator/s? Is S/he a data controller, as the Institution? Is he data processor, or something else?

The majority of scholars and practitioners in the field of GDPR compliance, have concluded that Arbitrator/s -like lawyers- is/are also data controller, playing that role, even as joint controller.[14] This means, that they have separate

[12] In case that they are collecting and processing data of European Union's citizens.
[13] GDPR applies to the activities of courts and judicial authorities (recital 20), and to the activities of lawyers (Recital 91).
[14] Art. 26 of GDPR.

accountability, though together with the Institutions as such, to prove compliance to certain requirements. Some of these obligations a data controller retains,[15] are:

the duty to inform the data subjects about the data process;[16]

the ability to provide certain procedures regarding the requests of data subjects for exercising their rights;[17]

the preparation of certain contracts of Article 28 GDPR *e. g.* for cloud service providers, accountants etc.;

also the preparation of certain Policies and Procedures and other documents;

the necessity of keeping records of processing activities due to Article 30 of GDPR;

the implement of certain technical measures, ensuring security of data[18] etc.

Supposing the Arbitrator/s, as independent actors – beyond Institutions, is a data controller, as a role, responsible for showing accountability, meaning compliance to GDPR, through all the above, and many more actions. Which is the responsibility of the, also data controller, as a role, Institution? How are Arbitrator/s and Institution connected? They shall be connected, due to European Regulation, and they have to be lawfully connected.

The answer is that: between Arbitrator/s and Institutions, shall be connected through an agreement regulating certain issues, that are imposed to be regulated by GDPR. What data will be collected and processed; for what purposes and on what legal ground will be processed; for how long and how the data will be retained (retention periods and territory); what the main responsibilities of the arbitrators and institutions as independent controllers will be, are the minimum issues shall be regulated in the above agreement.

The Legal Basis for a Lawful Process in ADR

GDPR has two paramount articles: 6 for data and 9 for special categories, known as "sensitive" categories of data. In those articles are described the legal reasons for a lawful data process, in every occasion. Unlawful process is forbidden and highly fined. One of the six legal basis, article 6, GDPR implies for lawful process of simple data, is the consent of data subjects. Consent is not the first basis, that data controller shall select, in fact is the last, when no other basis is suitable.

Consent is something that dominates also in ADR, because out of court procedures are consensus procedures, meaning the parties have to initiate them

[15] No matter if DC is a single person or A big company/organization/entity.
[16] Through documents as notices and privacy policies (Art. 12-14 of GDPR).
[17] Art. 15-22 of GDPR.
[18] Art. 32 of GDPR.

only if they want it and terminate them when they want it. At least in Mediation, because in Arbitration consensus and opt-out from courts willingness, counts only in the beginning mostly and in exceptional reasons effects in the termination. Nevertheless, ADR and GDPR acknowledge the notion of "consent". Unfortunately, though, in Arbitration consent is not the proper legal basis for processing data, that may include special categories of them. The reason is mainly, because the parties could not withdraw their given consent freely and at any time, just as easily they had given it.

The legal grounds, for a process of data, during Arbitration, may be the following:

the contract in which the Arbitration Clause is written;[19]

the legitimate interest of the Arbitrator and Institution;[20] and finally for some processes;

the legal obligation,[21] that data must be retained for standardized duration and for accounting purposes etc.

Especially the first reason, the contract, where is set Arbitration (or Mediation) Clause, shall be reformed in that manner that include that prediction.

The above mentioned legal basis, for a lawful simple data process, are selected due to the purposes of the data process. As far the special category of data, their processing is lawful, when it is "necessary for the establishment, exercise or defense of legal claims," as the "legal claims derogation". As a conclusion, Arbitral actors shall document in the beginning of arbitral proceedings what data shall be processed for the arbitration and the lawful basis that will be relied upon for the processing of any data, sensitive data or data related to children etc.

Strongly shall be kept in mind, that only the necessary data shall be processed even when there is a lawful basis. That obligation is the principles of both data minimization and purpose limitation. Also, in Arbitration shall not be forgotten the rights data subjects retain, and Arbitral actors shall provide:

data subject access request;

the right to request modification of their data, including the correction of errors and the updating of incomplete information;

the right to withdraw consent if consent was the basis for processing, which justifies why consent is risky to rely on as a lawful basis;

the right to object to processing;

the right to erasure.

[19] Art. 6(1)(b).
[20] Art. 6(1)(f).
[21] Art. 6(1)(c).

Concluding, accountability that GDPR implies, requires data controllers to take personal responsibility for data protection compliance and record the measures they take to comply with their data protection obligations. That accountability and compliance shall be not only when a case is registered in the Institution or in ad hoc Arbitration, or even to other ADR. All the above GDPR compliance shall be considered throughout the Arbitration or any ADR, even after decision making.

Especially, after proceedings are concluded, there is an anxiety of what happens to data, mostly sensitive data. Therefore, national law or legitimate interest of Arbitrators and Institutions, force them to retain data for the minimum time national Law imposes, *e. g.* for taxation reasons in Greece there Is an obligation to retain data 5 years after the case is closed.

GDPR and data protection in general is not in force for causing problems or putting obstacles to the procedures needed. Regulation is in force in order to help the lawful flow and transfer of data between persons and Institutions in order the private life of the subjects shall be protected. And that is a bet that ADR shall win (-win).

Instead of Epilogue

The issues that developed above and have considered practitioners and scholars, led International Council for Commercial Arbitration (ICCA) to collaborate with International Bar Association (IBA), and to publish a Roadmap to data protection in International Arbitration, in early 2020. This Roadmap develops a systematic approach of data protection in ADR procedures and especially in international Arbitration, analyses definitions, set roles and responsibilities of the actors of this institution and analyzes practical case-studies, showing in extension how GDPR Principles are protected in ADR mechanisms, like Principle of Lawful process, of Data minimization & Purpose limitation, of data security & subjects' rights, of transparency and of course accountability.

The complete analysis is approached for each stage of procedure. As there is Data flow from the beginning, when data are collected filing the Request for Arbitration, there shall be extended protection.

And as this Roadmap end, "there are sensible solutions to the data protection challenges that arise in arbitrations, and Arbitral Participants will soon become familiar with the issues and accustomed to dealing with them. The goal is to facilitate the process".

References

COURT OF JUSTICE OF THE EUROPEAN UNION (CJEU). *Handbook on European Data Protection Law*. Luxembourg: FRA/EctHR/EDPS, 2018.

RÜCKER, D.; KUGLER, T. (ed.) *New European General Data Protection Regulation*. A Practitioner's Guide. [*S. l.*]: Nomos/Hart, 2018.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

TSIPTSE, Olga N. EU Data Protection Regulation and How It Affects Arbitration and ADR-ODR. *Revista Brasileira de Alternative Dispute Resolution – RBADR*, Belo Horizonte, ano 03, n. 05, p. 195-202, jan./jun. 2021.