This article is from the American Review of International Arbitration (ARIA)
Vol. 30, No. 2 © JurisNet, LLC 2019 www.arbitrationlaw.com

USING ARBITRATION AND ADR FOR DISPUTES ABOUT PERSONAL AND NON-PERSONAL DATA: WHAT LESSONS FROM RECENT DEVELOPMENTS IN EUROPE?

*Jacques de Werra**

I. INTRODUCTION

The application of the General Data Protection Regulation (GDPR)[1] as of May 25, 2018, has provoked a flurry of reactions well beyond the territory of the European Union (as a result of the extensive territorial scope of the GDPR that can affect entities located outside of the European Union under certain conditions).[2] The GDPR has attracted a lot of attention and has also raised some concern in many business and legal communities, including the international arbitration community. The application of personal data law to the processing of personal data in the course of arbitration proceedings can be indeed quite complex (and potentially burdensome) and may impose additional obligations on the parties and (on the arbitral institutions) involved in the proceedings[3] that must be taken very seriously in view of the risks of liability resulting from the GDPR.

In spite of the importance of the application of the GDPR to international arbitration, it would be regrettable to consider that the new legal regimes regulating and protecting data (such as the GDPR) are only a source of concern for the global arbitration community. On the contrary, these legal regimes that create new legal obligations are likely to generate new legal challenges and legal disputes that could in turn be submitted to arbitration and to other alternative dispute resolution

* Professor of contract law and of intellectual property law at the University of Geneva School of Law (jacques.dewerra@unige.ch).

[1] Council Regulation 2016/679 of Apr. 27, 2016, 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), 2018, art. 79, O.J. (L 119/37) (EU), 80, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

[2] *See* Martin Zahariev, *Data Protection in Commercial Arbitration: In the light of GDPR* (Lambert Academic Publishing, 2019); Martin Zahariev, *GDPR Issues in Commercial Arbitration and How to Mitigate Them*, Kluwer Arbitration Blog, Sep. 7, 2019, *available at* http://arbitrationblog.kluwerarbitration.com/2019/09/07/gdpr-issues-in-commercial-arbitration-and-how-to-mitigate-them/. The International Council for Commercial Arbitration (ICCA) and the International Bar Association (IBA) have established the "ICCA-IBA Joint Task Force on Data Protection in International Arbitration Proceedings" (co-chaired by Kathleen Paisley and Melanie van Leeuwen – the author of this article is member of the task force) with the ambition to provide practical guidance on the potential impact of data protection principles, in particular the EU's General Data Protection Regulation (GDPR), on international arbitration proceedings, *see* https://www.arbitration-icca.org/projects/ICCA-IBA_TaskForce.html.

[3] *See* Kathleen Paisley, *It's All about the Data: The Impact of the EU General Data Protection Regulation on International Arbitration*, 41 FORDHAM INT'L L.J. 841 (2018).

mechanisms in certain circumstances. It is consequently not surprising that providers of arbitration and of other alternative dispute resolution (ADR) services have emerged in order to offer online dispute resolution tools for solving GDPR-related disputes (specifically for data breach disputes).[4] In any event, it is clear that in our data-driven economy in which data is and will be a key driver of innovation and power, the volume and strategic importance of "data disputes," generally defined as disputes relating to the conditions of protection, of access to and/or of use of data in certain circumstances will (continue to) increase significantly in the future.[5]

On this basis, the goal of this Article is to discuss the use of arbitration and of other alternative dispute resolution mechanisms for solving data disputes by focusing on certain types of data disputes that may result from regulatory instruments that have been adopted in the European Union.

Two preliminary comments must however be made: first, the use of arbitration for solving certain types of data disputes is not new. By way of illustration, the US Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA) provides for an arbitration system for defining under what (financial) conditions research data submitted by an applicant for registration of a new pesticide can be relied upon by a subsequent applicant.[6] FIFRA provides in this respect for a compulsory data licensing regime[7] through 7 U.S.C. § 136a(c)(1)(D)(ii) under which subsequent applicants for registration for a particular pesticide may use the original registrant's research data to obtain a so-called "'me-too' registration,"[8] provided that "the applicant has made an offer to compensate the original data submitter."[9] If the parties cannot agree on the "amount and terms of compensation," either party "may initiate binding arbitration proceedings."[10] In *Thomas v. Union Carbide*

---

[4] *See* Data Arbitration, https://dataarbitration.co.uk/ (offering an online "Data Arbitration scheme" in order to resolve personal data/GDPR-related disputes between consumers and companies that are signed up to their scheme). This raises the issue of the legal challenges of online arbitration (also from a GDPR/data protection perspective) that will not be discussed here, *see e.g.* the Report on Online Arbitration by the Working Group Chaired by Prof. Thomas Clay, le club de juristes, April 2019, *available at*: http://www.leclubdesjuristes.com/wp-content/uploads/2019/04/Online-Arbitration.pdf.

[5] Given that data can under certain conditions be protected by intellectual property law (and specifically by copyright and by trade secrets), and given that access to data and to information is frequently at the core of many intellectual property disputes, there is a strong convergence and proximity between the data disputes that are discussed here and intellectual property disputes relating to data / information; on this issue, *see* Jacques de Werra, *From Intellectual Property (Data-Related) Disputes to Data Disputes: Towards the Creation of a Global Dispute Resolution Ecosystem for Data Disputes in the Digital Era in* Resolving IP Disputes 87 (Gerold Zeiler & Alexander Zojer eds., 2018), *available at* https://archive-ouverte.unige.ch/unige:113027 (on which this Article is based).

[6] 7 U.S.C.S. § 136 et seq. (1982).

[7] Ruckelshaus v. Monsanto Co., 467 U.S. 986, 992 (1984).

[8] PPG Industries, Inc. v. Stauffer Chemical Co., 637 F. Supp. 85 (D.D.C. 1986).

[9] 7 U.S.C. § 136a(c)(1)(D)(ii).

[10] 7 U.S.C. § 136a(c)(1)(D)(ii).

Agricultural Products Co., 473 U.S. 568, [11] the U.S. Supreme Court confirmed the validity of this arbitration system: it held that the data-sharing and compensation system did not violate Article III, Section 1 of the U.S. Constitution.[12] This specific arbitration system tailored to one specific type of data disputes shows that arbitration is not a new phenomenon in the data dispute resolution ecosystem.

The second preliminary comment is that this Article will focus on disputes about data, i.e. on disputes in which the conditions of protection, access to and/or use of data are the very object of such dispute that shall be submitted to arbitration or other alternative dispute resolution mechanisms. This topic is different from the ones in which data-based and data-driven technological tools and other IT technologies (including big data, artificial intelligence, machine learning, etc.) are used for the purpose of supporting and facilitating the dispute resolution process (specifically in case of arbitration or other alternative dispute resolution mechanisms) and that shall not be discussed here.[13]

II. ARBITRATION AND ADR FOR DATA DISPUTES

Among the numerous types of data disputes that can be solved by arbitration and by other alternative dispute resolution mechanisms, this Article will focus on three types of data disputes: data portability disputes (see A below), personal date disputes under the Privacy Shield dispute resolution mechanism (see B below) and disputes about online intermediation services (see C below).

A. *Data Portability Disputes*

The portability of data is a major issue in the online digital environment. Online activities most frequently imply that clients (be there individuals or business clients) store their personal or non-personal data on data storage infrastructures made available by information service providers. Clients should in this respect have the opportunity to use another service provider and thus to transfer / migrate / port their data from their previous service provider to the new one without being hindered in this process. Different regulatory instruments facilitate the smooth migration and

---

[11] Thomas v. Union Carbide Agricultural Products Co., 473 U.S. 568; *see* John W. Navarra, *FIFRA Data-Cost Arbitration and the Judicial Power: Thomas v. Union Carbide Agricultural Products Co.: 105 S. Ct. 3325 (1985)*, 13 ECOLOGY L. QUARTERLY 609 (1986).

[12] *Thomas*, 473 U.S. at 568 ("Article III does not prohibit Congress from selecting binding arbitration with only limited judicial review as the mechanism for resolving disputes among participants in FIFRA's pesticide registration scheme").

[13] On this also quite challenging and most interesting topic, *see, e.g.* Arbitration in the Digital Age: The Brave New World of Arbitration (Maud Piers & Christian Aschauer eds., 2018); *Information Technology in International Arbitration*, ICC Commission on Arbitration and ADR, 2017, *available at* https://iccwbo.org/publication/information-technology-international-arbitration-report-icc-commission-arbitration-adr/; Gauthier Vannieuwenhuyse, *Arbitration and New Technologies: Mutual Benefits*, 35 J. OF INT'L ARBITRATION 119 (2018).

portability of data for the benefit of the clients by granting them certain rights to the portability of their data which depend on the type of data at issue and distinguish between non-personal data and personal data.

For non-personal data, the Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union of 14 November 2018 (hereinafter "the EU Non-Personal Data Regulation")[14] acknowledges that

> data mobility in the Union is also inhibited by private restrictions: legal, contractual and technical issues hindering or preventing users of data processing services from porting their data from one service provider to another or back to their own information technology (IT) systems, not least upon termination of their contract with a service provider.[15]

The EU Non-Personal Data Regulation further recognizes that "[t]he ability to port data without hindrance is a key factor in facilitating user choice and effective competition on markets for data processing services."[16] It further indicates that "professional users should be able to make informed choices and to easily compare the individual components of various data processing services offered in the internal market, including in respect of the contractual terms and conditions of porting data upon the termination of a contract."[17]

On that basis, the EU Non-Personal Data Regulation provides (in Article 6 entitled "Porting of data"[18]) that

> [t]he Commission shall encourage and facilitate the development of self-regulatory codes of conduct at Union level ('codes of conduct'), in order to contribute to a competitive data economy, based on the principles of transparency and interoperability and taking due account of open standards, covering, inter alia, the following aspects:
>
> > (a) best practices for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format including open standard formats where required or requested by the service provider receiving the data;
> > (b) minimum information requirements to ensure that professional users are provided, before a contract for data processing is concluded, with sufficiently detailed, clear and

---

[14] *See* Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018 O.J. (L 303) 59 (EU) [hereinafter EU Non-Personal Data Regulation].

[15] EU Non-Personal Data Regulation, *supra* note 14, Recital 5 at 60.

[16] EU Non-Personal Data Regulation, *supra* note 14, Recital 29 at 63.

[17] EU Non-Personal Data Regulation, *supra* note 14, Recital 30 at 63.

[18] EU Non-Personal Data Regulation, *supra* note 14, art. 6 at 67.

> transparent information regarding the processes, technical requirements, timeframes and charges that apply in case a professional user wants to switch to another service provider or port data back to its own IT systems … [19]

Pursuant to Article 6(2), "[t]he Commission shall encourage service providers to complete the development of the codes of conduct by 29 November 2019 and to effectively implement them by 29 May 2020."[20]

Interestingly, the EU Non-Personal Data Regulation does not impose or even propose any dispute resolution mechanism in case the data cannot be migrated from one provider to another. This is surprising because it can be expected that such disputes may arise relatively frequently between clients and their providers of IT services. The EU Non-Personal Data Regulation rather relies on the market and on self-regulation mechanisms (i.e., codes of conduct) to ensure that clients can effectively benefit from the mobility of their data.

Turning to data portability of personal data, Article 20(1) GDPR provides that

> [t]he data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: . . [21]

This provision confirms the existence of an enforceable right of individuals (data subjects) whose personal data are processed to obtain the portability of their data "without hindrance."[22] Article 20(2) GDPR further provides that "[i]n exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible."[23]

---

[19] *Id*.

[20] *Id.*

[21] GDPR, *supra* note 2, art. 20(1) at 45.

[22] For an analysis of the right to data portability, *See* Paul De Hert et al., *The right to data portability in the GDPR: Towards user-centric interoperability of digital services*, 34 COMPUTER LAW & SECURITY REV. 193 (2018); Barbara Van der Auwermeulen, *How to attribute the right to data portability in Europe: A comparative analysis of legislations*, 33 COMPUTER LAW & SECURITY REV. 57 (2017); Adrien Alberini & Yaniv Benhamou, *Data portability and interoperability : an issue that needs to be anticipated in today's IT-driven world*, Expert Focus (8/2017) 518-523; *see also*, Data Prot. Working Party, *Guidelines on the right to data portability*, art. 29, 16/EN, WP242rev.01 (Dec. 13, 2016), *available at* http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

[23] GDPR, *supra* note 2, art. 20(2) at 45.

Article 20(4) GDPR also provides that "[t]he right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others."[24]

These references to third parties, and specifically to the new controller, show that bilateral disputes may also involve the interests and positions of third parties. Similarly to disputes relating to the portability of non-personal data, it is likely that the exercise of the right of portability of personal data will generate many disputes. This right is enforceable pursuant to the relevant provisions of the GDPR. On this basis, the data subject shall first make a request for data portability to the controller.[25] Based on Article 12(3) GDPR, "[t]he controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request."[26] Article 12(4) GDPR further provides that "[i]f the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy."[27] Based on Article 77(1) GDPR, the right of the data subject to lodge a complaint with a supervisory authority is "[w]ithout prejudice to any other administrative or judicial remedy." With respect to judicial remedy, Article 79(1) GDPR provides that "[w]ithout prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation."[28] It can be assumed that disputes about the right to data portability under Article 20 GDPR shall fall under this provision, even though it may be uncertain, based on the wording of Article 79(1) GDPR, that the right to data portability under Article 20 is infringed "as a result of the processing of his or her personal data in non-compliance with this Regulation."[29]

---

[24] *Id*.

[25] The controller must inform the data subjects about the existence of their right to data portability (*see* GDPR, *supra* note 2, arts. 13(2)(b) & 14(2)(c) at 41-42) along with information about the other rights of the data subjects.

[26] GDPR, *supra* note 2, art. 12(3) at 40.

[27] This provision does not seem to cover the case in which the controller would react positively to the request to data portability but would not do so in a satisfactory way from the standpoint of the data subject. In such a case, it seems reasonable to admit that the data subject shall also have the right to initiate legal action against the controller.

[28] GDPR, *supra* note 2, art. 79(1). *See also* GDPR, art. 79(2) at 80 (stating that "[p]roceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers").

[29] GDPR, *supra* note 2, art. 79(1). Unless it shall be considered that the actions that are accomplished or not accomplished (because the data subject could complain about the

In any event, it is interesting to point out that Article 79(1) GDPR expressly reserves "any non-judicial remedy,"[30] thereby showing the potential importance of this type of remedy for enforcing the rights of data subjects under the GDPR. In this respect, Article 40(1) GDPR encourages "the drawing up of codes of conduct intended to contribute to the proper application of this Regulation,"[31] by providing more specifically in Article 40(2) GDPR that

> [a]ssociations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to: . . . .
>
> . . . .
>
> (k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.[32]

It may be uncertain (similarly to what was noted above with respect to the wording of Article 79(1) GDPR) that Article 40(2)(k) GDPR (based on its wording) covers disputes about the right to data portability (unless the actions – or the inactivity – of the controller with respect to the portability of data to another controller amount to processing of data). In any case, it seems important to consider alternative dispute resolution mechanisms because such mechanisms could significantly help ensure the effective enforceability of the right to data portability and could also reduce the caseload that may affect or even paralyze both administrative (i.e. supervisory authority) and judicial bodies if they were to be massively seized with numerous requests of data portability. As this is the case for many other disputes in the online environment, traditional judicial or administrative proceedings may not necessarily constitute an adequate solution because of the high cost and length of such proceedings.

In a data-driven online environment in which data mobility is key, disputes about data portability are likely to arise massively in the future. This calls for the development of effective dispute resolution mechanisms for disputes arising about data mobility. This should be achieved in a coordinated manner in order to avoid

---

inactivity of the controller who will not make the data available for portability) by the data controller with the view to prepare and facilitate the data portability to another controller amount to "processing" within the meaning of GDPR Article 2(2). *See* GDPR, *supra* note 2, art. 2(2) at 32 (defining processing as 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).

[30] GDPR, *supra* note 2, art. 79(1) at 80.

[31] *Id.*, art. 40(1) at 56.

[32] *Id.*, art. 40(2) at 56-57.

the fragmentation of disputes, even if the right to data portability may result from different regulatory sources. On this basis, it would be helpful to develop uniform alternative dispute resolution mechanisms in order to ensure the enforceability and effectiveness of the right to data portability for personal as well as for non-personal data. The need for coordination between the regulatory regimes respectively applicable to personal and non-personal data is essential knowing that in practice datasets will very frequently consist of both personal and non-personal data (mixed datasets). The EU institutions were well aware of the risks of the diverging regulatory treatment governing personal and non-personal data at the time of adoption of the EU Non-Personal Data Regulation. On this basis, the European Commission was instructed to publish by 29 May 2019 "informative guidance on the interaction of this Regulation and Regulation (EU) 2016/679, especially as regards data sets composed of both personal and non-personal data".[33] This resulted in the issuance of the "Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union" by the European Commission on 29 May 2019.[34] The Guidance provides that there "are no contradictory obligations" under the GDPR and the EU Non-Personal Data Regulation[35] and that "[i]n most real-life situations, a dataset is very likely to be composed of both personal and non-personal data [which constitutes a mixed dataset]".[36] The Guidance further identifies situations where the porting of data would be covered by both the GDPR and the EU Non-Personal Data Regulation.[37] The Guidance however does not define how to solve disputes which may emerge about data portability in a coherent and concerted manner. It will be interesting to observe whether this issue will be addressed in the upcoming self-regulations (codes of conduct) that shall be adopted and / or in the model contractual clauses that shall be made available (and that could provide for ADR / arbitration dispute resolution mechanisms).[38]

In addition to the Guidance, Art. 8 para. 1 of the EU Non-Personal Data Regulation provides that

> [n]o later than 29 November 2022, the Commission shall submit a report to the European Parliament, to the Council and to the European Economic and Social Committee evaluating the implementation of this Regulation, in particular in respect of: (a) the application of this Regulation, especially to data sets composed

---

[33] EU Non-Personal Data Regulation, *supra* note 14, art. 8, ¶ 3.

[34] Communication from the Commission to the European Parliament and the Council, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union of 29 May 2019 (COM/2019/250 final), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN (it is important to emphasize that this document expressly indicates that it "is provided by the European Commission for information purposes only.").

[35] Guidance, *supra* note 34, at 4.

[36] *Id*.

[37] *Id*.

[38] *Id*; *see also*, the EU Non-Personal Data Regulation, *supra* note 14, recital 30.

> of both personal and non-personal data in the light of market developments and technological developments which might expand the possibilities for deanonymising data . . . .[39]

In any event, it appears important to develop dispute resolution mechanisms that shall help solve transnational data portability disputes.

From this perspective, the question arises whether disputes between controllers and data subjects with regard to processing could validly be submitted to arbitration. This could be based on an arbitration clause that would bind the controller and the data subjects. The title ("Right to an effective judicial remedy against a controller or processor") and the wording of Art. 79 GDPR may seem to indicate that the "right to an effective judicial remedy" is mandatory and unwaivable and thus cannot be waived by submitting disputes to arbitration ("each data subject shall have the right to an effective judicial remedy").[40] This is also reflected in art. 40 para. 2(k) of the GDPR exposing that codes of conduct for the purpose of specifying the application of this Regulation can regulate "out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, *without prejudice to the rights of data subjects pursuant to Articles 77 and 79*."[41] (italics added).

However, it is reasonable to consider that the parties in disputes, i.e. the controllers and the data subjects, shall have the freedom and autonomy to decide to solve their personal data dispute by submitting it to a "non-judicial remedy"[42] and specifically to arbitration. The "right to an effective judicial remedy" reflects the "right to an effective remedy" anchored in Art. 47 of the EU Charter of Fundamental Rights which provides that "[e]veryone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article." This provision and "the right to an effective remedy before a tribunal" that it reflects do not prevent the submission of a dispute to alternative dispute resolution mechanisms and specifically to arbitration.[43]

There is no indication that data disputes under the GDPR are generally and by their very nature non-arbitrable subject matters. This can be confirmed by the setting up of the dedicated arbitration mechanism designed and approved by the EU in the Privacy Shield system (see infra B) which would not be conceivable if the EU position was that this type of personal data disputes would not be (objectively) arbitrable. As a result, data disputes arising between data processors or data

---

[39] EU Non-Personal Data Regulation, *supra* note 14, art. 8(1), at 68.

[40] *See* GDPR, *supra* note 2, art. 79(1), 80.

[41] *Id*., art. 40 para. 2(k), at 80.

[42] *Id*., art. 78 para. 1-2, at 57.

[43] *See*, *e.g.*, European Union Agency for Fundamental Rights, Handbook on European Law Relating to Justice, 48 (2016) *available at* https://www.echr.coe.int/Documents/Handbook_access_justice_ENG.pdf. ("Alternative dispute resolution (ADR) procedures, such as mediation and arbitration, provide alternatives to accessing justice via formal judicial routes.").

controllers and data subjects that are governed by the GDPR should be arbitrable. This should particularly be the case for disputes falling within the scope of Art. 82 providing for a right to compensation and liability.[44] Art. 82 para. 1 GDPR provides that "[a]ny person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."[45] With respect to material damages, no manifest public interest should prevent the submission of monetary disputes (leading to material damages) to arbitration. The issue might appear more complex with claims for non-material damage which are also covered by Art. 82 para. 1 GDPR.[46] However, even for claims relating to non-material damage, there is no compelling reason why such claims should not be arbitrable either as a matter of principle.[47]

It should also be noted that Art. 82 para. 6 GDPR identifies the national courts before which the legal action shall be initiated by providing that "[c]ourt proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2)." This provision should however not prevent the submission to arbitration of a dispute about the right to receive compensation for the damages suffered because Art. 82 para. 6 (logically) only refers to court proceedings and does not as such exclude the use of alternative dispute resolution mechanisms for solving this type of disputes.

B. *Privacy Shield Disputes*

A dedicated arbitration system which is managed by the American Arbitration Association (AAA)'s International Center for Dispute Resolution (ICDR)[48] has also been created and implemented under the Privacy Shield system.[49]

It should be noted from the outset that the future of the Privacy Shield system (and thus of the Privacy Shield arbitration system) is uncertain in view of the

---

[44] *See* GDPR, *supra* note 2, art. 82.

[45] *Id*., art. 82(1).

[46] *Id*.

[47] By analogy, moral rights disputes are generally considered to be arbitrable even if they relate to personal / non-commercial interests of authors of copyright-protected works. *See e.g*. Desputeaux v. Éditions Chouette (1987) Inc., [2003] S.C.R. 178 (Can.), *available at* https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2048/index.do.

[48] *See* EU-U.S. Privacy Shield, Annex I: Binding Arbitration Mechanism, AMERICAN ARBITRATION ASSOCIATION, *available at* http://go.adr.org/privacyshieldannex.html; ICDR-AAA EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Program Independent Recourse Mechanism (IRM), ARBITRATION MECHANISM AMERICAN ARBITRATION ASSOCIATION, *available at* http://go.adr.org/privacyshield.html (this paper will not analyze in detail this arbitration system; it will not discuss either the so-called Independent Recourse Mechanism (IRM) that has also been created under the Privacy Shield system.).

[49] *See* U.S. DEP'T OF COMMERCE, E.U.-U.S. Privacy Shield Framework Principles, Annex I (Introduction) (2016), *available at* https://www.privacyshield.gov/article?id =ANNEX-I-introduction.

judicial challenges that it faces[50] and also in light of the application of the GDPR, which has led to a resolution adopted by the European Parliament calling for the suspension of the EU-US Privacy Shield on the ground that the Privacy Shield would not comply with the (now enhanced) EU standard of protection of personal data resulting from the GDPR.[51] For this reason, the Privacy Shield arbitration mechanism may not necessarily be promised to a bright future. It should further be noted that, in any event, the Privacy Shield arbitration system can be used only provided that various (potentially burdensome) pre-arbitration mechanisms have been initiated (and exhausted) by the individuals before they can submit their dispute to arbitration (which can significantly reduce the importance and relevance of this arbitration system in practice).[52]

In spite of this, the Privacy Shield arbitration mechanism remains interesting to observe because it shows the benefits that arbitration and alternative dispute

---

[50] This depends on the outcome of the so-called "Schrems II" case (named after the data protection/privacy Austrian activist who litigated against Facebook in a high-profile data protection/privacy dispute which was ultimately submitted to the Court of Justice of the European Union (Case C-362/14, judgment of October 6, 2015, which is the "Schrems I" case). The Schrems II case is pending before the CJEU (case C-311/18) which held a hearing on July 9, 2019, *see* Jennifer Baker, *CJEU's hearing on Schrems II has both sides worried ruling could be sweeping*, IAPP, July 9, 2019, *available at* https://iapp.org/news/a/cjeus-hearing-on-schrems-ii-has-both-sides-worried-ruling-could-be-sweeping/; another case dealing more directly with the validity of the Privacy Shield system, Case T-738/16, Quadrature du Net v. European Commission, has been suspended pending the resolution of Case C-311/18; *see* Jennifer Baker, *EU High Court hearings to determine future of Privacy Shield, SCCs*, IAPP, June 25, 2019, *available at* https://iapp.org/news/a/eu-high-court-hearings-to-determine-future-of-privacy-shield-standard-contractual-clauses/.

[51] *See* Resolution 2018/2645 of the European Parliament of 5 July 2018 on the Adequacy of the Protection Afforded by the EU-US Privacy Shield, *available at* http://www.euro parl.europa.eu/doceo/document/TA-8-2018-0315_EN.html?redirect. (under this resolution, the European Parliament (among other points) "Takes the view that the current Privacy Shield arrangement does not provide the adequate level of protection required by Union data protection law and the EU Charter as interpreted by the CJEU; 35. Considers that, unless the US is fully compliant by 1 September 2018, the Commission has failed to act in accordance with Article 45(5) GDPR; calls therefore on the Commission to suspend the Privacy Shield until the US authorities comply with its terms"); for a comment, *see* Natasha Lomas, *EU parliament calls for Privacy Shield to be Pulled Until US Complies*, TECHCRUNCH, July 5, 2018, https://techcrunch.com/2018/07/05/eu-parliament-calls-for-privacy-shield-to-be-pulled-until-us-complies/; the Privacy Shield is however still applicable as of the writing of this Article; it is subject to annual reviews, *see* the Joint Press Statement from Commissioner Věra Jourová and Secretary of Commerce Wilbur Ross on the Third Annual EU-U.S. Privacy Shield Review (Sept. 13, 2019) *available at*: https://ec.europa.eu/commission/presscorner/detail/en/statement_19_5563; the reports on the first and on the second reviews are *available at* https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

[52] *See* U.S. DEP'T OF COMMERCE, E.U.-U.S. Privacy Shield Framework Principles, C. Pre-Arbitration Requirements (2016), *available at* https://www.privacyshield.gov/article?id=C-Pre-Arbitration-Requirements.

resolution mechanisms more generally can offer for solving transnational personal data disputes. The arbitration system that is established under the Privacy Shield has a limited scope because it can only offer "non-monetary equitable remedy" and thus expressly excludes any damages,[53] whereby damages could be claimed in other fora.[54] This however does not mean that the system would not have any relevance knowing that other alternative dispute resolution mechanisms under which damages are also excluded have proven to be extremely useful for the stakeholders and to be most successful in practice. This is notably the case of the Uniform Domain Name Dispute Resolution Policy (UDRP)[55] that was adopted for solving Internet domain name cybersquatting disputes. Even if the UDRP remains an *alternative* dispute resolution mechanism that was not designed to replace court proceedings, it is worth noting that the UDRP has progressively become the go to dispute resolution mechanism for solving international domain name-related trademark disputes.[56] On this basis, and even if no damages can be granted under

---

[53] *Id*., B. Available Remedies, *available at* https://www.privacyshield.gov/article?id=B-Available-Remedies ("Under this arbitration option, the Privacy Shield Panel (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question) necessary to remedy the violation of the Principles only with respect to the individual. These are the only powers of the arbitration panel with respect to remedies. In considering remedies, the arbitration panel is required to consider other remedies that already have been imposed by other mechanisms under the Privacy Shield. No damages, costs, fees, or other remedies are available. Each party bears its own attorney's fees.").

[54] *Id*., D. Binding Nature of Decisions, *available at* https://www.privacyshield.gov/article?id=D-Binding-Nature-of-Decisions ("An individual's decision to invoke this binding arbitration option is entirely voluntary. Arbitral decisions will be binding on all parties to the arbitration. Once invoked, the individual forgoes the option to seek relief for the same claimed violation in another forum, except that if non-monetary equitable relief does not fully remedy the claimed violation, the individual's invocation of arbitration will not preclude a claim for damages that is otherwise available in the courts.").

[55] *See* ICANN, Uniform Domain Name Dispute Resolution Policy, Internet Corp. for Assigned Names and Numbers, https://www.icann.org/resources/pages/help/dndr/udrp-en (last visited Nov. 10, 2019).

[56] From this perspective, the UDRP constitutes a very interesting example showing the importance of alternative dispute resolution mechanisms for solving international intellectual property disputes. This relates to the discussion taking place in the legal literature promoting the use of alternative dispute resolution mechanisms as default rules for international intellectual property disputes. *See* Jacques de Werra, *Can Alternative Dispute Resolution Mechanisms Become the Default Method for Solving International Intellectual Property Disputes?*, 43 CAL. W. INT'L L.J. 39 (2012) *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2195968; *see also* Gilles Cuniberti, *Rethinking International Commercial Arbitration: Towards Default Arbitration*, TRANSNATIONAL DISPUTE MANAGEMENT, Feb. 9, 2017, *available at* https://www.transnational-dispute-management.com/journal-advance-publication-article.asp?key=1700 (in which the author discusses the case of intellectual property disputes (in light of the above mentioned article written by the author of this Article).

the UDRP, the UDRP is and remains of key value for all stakeholders. This is confirmed by the record-breaking number of cases brought before the WIPO Mediation and Arbitration Center (which is the most important platform offering UDRP and other Internet domain name dispute resolution services) for domain name disputes in 2017[57] and 2018[58], twenty years after the adoption and implementation of the UDRP (in 1999).

C. *Disputes about Online Intermediation Services*

Another source of data-related disputes in the EU will result from the EU regulation on promoting fairness and transparency for business users of online intermediation services that was recently adopted by the relevant EU bodies[59] (hereafter the "EU Online Intermediation Regulation").[60] The variety of disputes that will emerge from this regulation go beyond data disputes (on which this Article focuses): data disputes are however of high relevance in the EU Online Intermediation Regulation as reflected in the statement made therein according to which "[t]he ability to access and use data, including personal data, can enable important value creation in the online platform economy, both generally as well as for the business users and online intermediation services involved"[61]. Art. 9 of the EU Online Intermediation Regulation specifically regulates a right of "access to data" by providing that "[p]roviders of online intermediation services shall include in their terms and conditions a description of the technical and contractual access, or absence thereof, of business users to any personal data or other data, or both, which business users or consumers provide for the use of the online intermediation services concerned or which are generated through the provision of those services" (art. 9 para. 1).[62] The obligation of information of the providers of online intermediation services to their business users shall include whether the "personal data or other data, or both, which business users or consumers provide for the use of [the online intermediation] services or which are generated through the provision of those services" (art. 9 para. 2 (a) is shared with third parties (art.

---

[57] *See WIPO Cybersquatting Cases Reach New Record in 2017*, WIPO (Mar. 14, 2018) *available at* http://www.wipo.int/pressroom/en/articles/2018/article_0001.html.

[58] *See WIPO Cybersquatting Cases Grow by 12% to Reach New Record in 2018*, WIPO (March 15, 2019), *available at* https://www.wipo.int/pressroom/en/articles/2019/article_0003.html.

[59] *See* European Commission Press Release IP/19/1168, The Commission, Digital Single Market: EU Negotiators Agree to Set Up New European Rules to Improve Fairness of Online Platforms' Trading Practices (February 14, 2019), *available at* https://europa.eu/rapid/press-release_IP-19-1168_en.htm.

[60] Regulation 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, 2019 O.J. L 186/57 (EU), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R1150&from=EN.

[61] EU Online Intermediation Regulation, *supra* note 60, Recital 33.

[62] *Id.*, at art. 9(1).

9 para. 2 (d)).[63] On this basis, and in view of the commercial (and financial) importance of data sharing (and of data sharing agreements) and of "derived data"[64] in today's and tomorrow's data-driven business world, it is very likely that disputes will arise about the validity and scope of data sharing under the EU Online Intermediation Regulation. It can therefore be expected that the EU Online Intermediation Regulation will generate a significant volume of data disputes.

The EU Online Intermediation Regulation aims at protecting business users of online intermediation services[65] against various activities which include the unilateral changes of terms of services, the suspension or termination of the business users' accounts and the conditions under which rankings are made by providers of online intermediation services and by providers of online search engines[66] (with obligations of transparency, non-discrimination etc.). In terms of territorial scope, the EU Online Intermediation Regulation

> shall apply to online intermediation services and online search engines provided, or offered to be provided, to business users and corporate website users, respectively, that have their place of establishment or residence in the Union and that, through online intermediation services or online search engines, offer goods or services to consumers located in the Union, irrespective of the place of establishment or residence of the providers of those services and irrespective of the law otherwise applicable.[67]

In addition to substantive rights granted to business users, the EU Online Intermediation Regulation provides for various procedural mechanisms that

---

[63] *Id*., at art. 9(2).

[64] *See* Henry Lebowitz, Jeffrey P. Cunard, Jonathan E. Levitsky, Michael Schaper, Michael A. Diz & Jim Pastore, *Derived Data: Contracting Considerations and Market Practices*, Debevoise & Plimpton (Aug. 30, 2018), *available at* https://www.debevoise.com/~/media/files/insights/publications/2018/08/201808_tmt_insights_august_2018.pdf.

[65] *See* EU Online Intermediation Regulation, *supra* note 60, art. 2(2) ("Online intermediation services" are defined in Article 2(2) as "services which meet all of the following requirements: (a) they constitute information society services within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council; (b) they allow business users to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded; (c) they are provided to business users on the basis of contractual relationships between the provider of those services and business users, which offer goods or services to consumers.").

[66] *Id*., at art. 2(5) (Article 2(5) defines "online search engine" as "digital service that allows users to input queries in order to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found.")

[67] *Id*., at art. 1(2).

ambition to offer efficient remedies to business users of online intermediation services that were not available until then.[68]

The dispute resolution mechanisms that are available in the EU Online Intermediation Regulation build together a multi-track dispute resolution mechanism that is composed of an internal / easily accessible system for handling the complaints of business users (Article 11), of a mediation (Article 12) and of judicial proceedings (Article 15).[69] In view of the costs of setting up and maintaining these dispute resolution mechanisms, the EU Online Intermediation Regulation provides that they are not imposed on providers of online intermediation services that are small enterprises as defined under EU law.[70] Interestingly, the "internal" complaint-handling system does not need to be fully internal given that a delegation to an "external service provider or other corporate structure" is possible "as long as the operator has full authority and the ability to ensure compliance of the internal complaint-handling system with the requirements in this Regulation"[71].

The internal complaint-handling system is generally designed to handle "the complaints of business users" (Art. 11 para. 1).[72] The EU Online Intermediation Regulation specifically provides that the internal complaint-handling system can apply with respect to the protection of business users against the restriction, suspension or termination of the provision of its online intermediation services unilaterally decided by the provider of such services (Art. 4).[73] Art. 4 para. 3 provides that "[i]n the case of restriction, suspension or termination, the provider of online intermediation services shall provide the business user the opportunity to clarify the facts and circumstances in the framework of the complaint handling process referred to in Article 11" (art. 4 para. 3).[74] In view of the significant impact of the risk of a restriction, a suspension or - even more significantly - of a termination, the business user should keep the possibility to initiate formal judicial

---

[68] *See Commission Factsheet on Online Platforms: New Rules to Increase Transparency and Fairness*, COM (Feb. 14, 2019), *available at* https://ec.europa.eu/digital-single-market/en/news/online-platforms-new-rules-increase-transparency-and-fairness (the problems that have been identified by the European Commission in terms of remedies that the EU Online Intermediation Regulation is designed to tackle are: Lack of redress as 1/3 of all P2B problems remain unsolved and 1/3 are solved with difficulties business users are faced with: Platforms' inexistent or ineffective internal complaint handling mechanisms, Inexistent specialized and effective external, out of court redress mechanisms, Limited and costly access to EU Courts).

[69] *See* EU Online Intermediation Regulation, *supra* note 60, arts. 11, 12 and 15.

[70] *Id.*, at art. 11(5) and art. 12 (7) (providing that certain obligations shall not apply to providers of online intermediation services that are small enterprises within the meaning of Article 2 (2) of the Annex to Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, 36)).

[71] *Id*., at 65.

[72] *Id*. art. 11(1).

[73] *Id*. art. 4.

[74] *Id*. art. 4(3).

proceedings (including by requesting temporary injunctions) against the provider in order to keep access to the relevant services. Art. 4 para. 2 of the EU Online Intermediation Regulation gives to the business user a notice period of at least 30 days in case the provider of online intermediation services shall decide to terminate the provision of the whole of its online intermediation services to a given business user, whereby the provider shall also notify the statement of reasons for that decision on a durable medium.[75] However, this notice period will most likely not be sufficient for the business user to find adequate (alternative) solutions.

On this basis, the business user shall not be restrained in the legal remedies and enforcement mechanisms that it can choose and shall not be obliged to first submit to the internal complaint-system before initiating formal judicial proceedings.

The categories of disputes that can be submitted to the internal complaint-handling system are defined in Art. 11 para. 1 and cover (as exhaustively defined):

> (a) alleged non-compliance by that provider with any obligations laid down in this Regulation which affects the complainant;
> (b) technological issues which relate directly to the provision of online intermediation services, and which affect the complainant
> (c) measures taken by, or behaviour of, that provider which relate directly to the provision of the online intermediation services, and which affect the complainant.[76]

Based on this wording, it appears that not "any disputes between the provider and the business user arising in relation to the provision of the online intermediation services concerned" (which is the wording of the scope of the disputes that can be submitted to mediation under Art. 12 para. 1) can be submitted to the internal complaint-handling system.[77] Quite to the contrary, only the disputes that fall within (at least) one of the three (relatively narrow) categories can be submitted to such system. It is however not optimal and fully coherent that the scope of the disputes submitted to the internal complaint-handling system is narrowly defined and does not correspond to the disputes that can be submitted to mediation. The restriction to the "non-compliance by that provider with any obligations laid down in this Regulation which affects the business user lodging the complaint"[78] does not appear adequate because it is likely that disputes may arise about other terms and conditions / contractual issues in the relationships between providers and users that would not necessarily correspond to "obligations laid down in this Regulation"

---

[75] *Id*. art. 4(2); art. 2(13) (The "durable medium" being defined as "any instrument which enables business users to store information addressed personally to them in a way accessible for future reference and for a period of time adequate for the purposes of the information and allows the unchanged reproduction of the information stored.").

[76] *Id*. art. 11(1).

[77] *Id*. art. 12(1).

[78] *Id*. art. 11(1)(a).

(such as financial terms and conditions).[79] The efficiency of dispute resolution mechanisms and the interest to centralize disputes before one dispute resolution body would plead for a more comprehensive and more extensive approach similarly to what is reflected in the scope of the mediation services that shall encompass any disputes between the provider and the business user arising in relation to the provision of the online intermediation services concerned. It would thus make sense that the "jurisdictional" scope of the disputes / complaints that can be submitted to the internal complaint-handling system shall cover all types of disputes that could then be submitted to mediation. This would make sense also because Art. 12 para. 2 provides that the mediation can cover "complaints that could not be resolved by means of the internal complaint-handling system referred to in Article 11".[80]

The internal complaint-handling system imposed on the providers of online intermediation shall be easily accessible and free of charge for business users and shall ensure handling within a reasonable time frame (Article 11 para. 1). It also requires that the providers shall communicate to the complainant the outcome of the internal complaint-handling process in an individualized manner and in plain and intelligible language (Article 11 para. 2 (c)) and that they shall make easily available to the public information on the functioning and effectiveness of their internal complaint-handling system, including the number of complaints lodged, the main types of the complaints, the average time period needed to process the complaints and aggregated information regarding the outcome of the complaints (Article 11 para. 4).

With respect to mediation,[81] providers of online intermediation services shall have the obligation to "identify in their terms and conditions two or more mediators with which they are willing to engage to attempt to reach an agreement with business users on the settlement, out of court, of any disputes between the provider and the business user arising in relation to the provision of the online intermediation services concerned […]" (Article 12 para. 1).[82]

Interestingly and perhaps regrettably, this provision only refers to the identification of (two or more) mediators and does not refer to any mediation rules that shall be applicable (even if reference to mediation rules are common and useful in order to ensure the streamlined organization of the mediation process, in reflected in many institutional mediation rules). It remains to be seen how this will be applied in practice. The specific rules that shall apply to the mediation process as well as to the internal complaint system (beyond the general and undetailed principles that are

---

[79] *Id*.

[80] *Id*. art. 12(2).

[81] It being reminded that the Directive 2008/52/EC of 21 May 2008 on certain aspects of mediation in civil and commercial matters promotes the use of mediation at the EU level; the EU Online Intermediation Regulation refers to it by defining "mediation" as "any structured process as defined in point (a) of Article 3 of Directive 2008/52/EC," EU Online Intermediation Regulation, *supra* note 60, art. 2 (12).

[82] Specific conditions are also set forth in Article 12(2) with respect to the requirements imposed on the mediators (including and starting with impartiality and independence).

mentioned in the EU Online Intermediation Regulation) will have to be defined. This might be done in the codes of conduct that shall be drawn up

> by providers of online intermediation services and by organisations and associations representing them, together with business users including SMEs and their representative organisations, that are intended to contribute to the proper application of this Regulation, taking account of the specific features of the various sectors in which online intermediation services are provided, as well as of the specific characteristics of SMEs.[83]

In spite of this, the EU Online Intermediation Regulation still contains certain rules about the mediation. Pursuant to Article 12 para. 3, "[n]otwithstanding its voluntary nature, providers of online intermediation services and business users shall engage in good faith throughout any mediation attempts conducted pursuant to this Article". In terms of costs, a "reasonable proportion of the total costs of mediation" shall be borne by the providers of online intermediation services (Article 12 para. 4). The providers are further encouraged to "individually or jointly, set up one or more organisations providing mediation services […] for the specific purpose of facilitating the out-of-court settlement of disputes with business users arising in relation to the provision of those services, taking particular account of the cross-border nature of online intermediation services" (Article 13). The need to develop specialized mediation services and to involve specialized mediators is justified because

> [t]he involvement of mediators having specialist knowledge of online intermediation services as well as of the specific industry sectors within which those services are provided should add to the confidence both parties have in the mediation process and should increase the likelihood of that process leading to a swift, just and satisfactory outcome.[84]

This is an important statement confirming the importance of having specialized providers of dispute resolution services that shall have a sufficient level of expertise in the relevant digital online markets and industries.

In terms of judicial proceedings, the EU Online Intermediation Regulation clarifies that any attempt to reach an agreement through mediation "shall not affect the rights of the providers of online intermediation services and of the business users concerned to initiate judicial proceedings at any time before, during or after the mediation process" (Article 12 para. 5).

---

[83] *See* EU Online Intermediation Regulation, *supra* note 60, art.17(1).

[84] *See* EU Online Intermediation Regulation, *supra* note 60, Recital 43.

It further contains a provision reinforcing the protection of business users by enabling organizations representing business users or corporate website users to take legal action. Article 14 para. 1 provides that

> [o]rganisations and associations that have a legitimate interest in representing business users or in representing corporate website users, as well as public bodies set up in Member States, shall have the right to take action before competent national courts in the Union, in accordance with the rules of the law of the Member State where the action is brought, to stop or prohibit any non-compliance by providers of online intermediation services or by providers of online search engines, with the relevant requirements laid down in this Regulation.

This approach (which is common under consumer law but not in a business to business (B2B) context) aims at ensuring the effective compliance by providers of online intermediation services and by providers of online search engines with their obligations under the EU Online Intermediation Regulation, given that individual court proceedings initiated by business users may not constitute a viable solution.[85]

As resulting from the preceding paragraphs, the EU Online Intermediation Regulation regulates or at least provides for three different types of dispute resolution mechanisms for disputes arising between business users and providers of online intermediation services: the internal complaint-handling system, mediation and judicial proceedings. It however does not mention any other dispute resolution mechanism and surprisingly does not refer at all to arbitration. This is regrettable because arbitration probably constitutes the most established and privileged dispute resolution mechanism for solving cross-border commercial disputes. Arbitration thus appears as an attractive tool for solving the types of disputes that may arise between business users and providers of online intermediation services under the EU Online Intermediation Regulation.

Even if one can speculate about the reason(s) why there is no reference to arbitration in the EU Online Intermediation Regulation (perhaps because of certain reluctance against arbitration),[86] it remains that the parties should be in a position to submit their disputes with the providers of such services to trusted neutral and independent expert arbitrators that could validly decide on such disputes in the course of arbitration proceedings. Nothing in the EU Online Intermediation Regulation seems to prevent the use of arbitration for solving these disputes as a

---

[85] EU Online Intermediation Regulation, *supra* note 60, Recital 44 provides that various factors, such as limited financial means, a fear of retaliation and exclusive choice of law and forum provisions in terms and conditions, can limit the effectiveness of existing judicial redress possibilities, particularly those which require business users or corporate website users to act individually and identifiably.

[86] This could have a particular weight in consumer disputes, and has a lower relevance for corporate disputes.

matter of principle. Art. 8 of the EU Online Intermediation Regulation identifies three categories of specific contractual terms that must be scrutinized in "order to ensure that contractual relations between providers of online intermediation services and business users are conducted in good faith and based on fair dealing", none of which relates to ADR / arbitration. The EU Online Intermediation Regulation however imposes that the Regulation shall be submitted to regular evaluations by the European Commission that should "include the effects on business users which may result from the general use of exclusive choice of law and forum provisions in terms and conditions which are unilaterally determined by the provider of the online intermediation services" (recital 49). The scrutiny of "exclusive choice of law and forum provisions" might also indirectly include arbitration clauses (or other ADR clauses) that could be included in the terms and conditions of providers of online intermediation services. This however does not imply that arbitration should be more scrutinized than exclusive choice of court clauses that would confer exclusive jurisdictional power to foreign (non-EU-based) courts and would thus deprive business users from accessing EU courts.

The submission to arbitration could be achieved on the basis of an arbitration clause to be inserted in the agreements between the platforms offering online intermediation services and their business users. The EU Online Intermediation Regulation somewhat imprecisely indicates that "[p]roviders of online intermediation services shall identify in their terms and conditions two or more mediators" (art. 12 para. 1). In line with standard commercial ADR practice, these agreements could include a mediation clause (rather than identifying "two or more mediators" – this wording raises the question of which one of the two or more meditators shall mediate the dispute, knowing that a mediation with more than one mediator is not usual). Multi-tier dispute resolution clauses could also come into consideration, and specifically mediation-arbitration (med-arb) clauses. The EU Online Intermediation Regulation could thus have indicated that mediation and arbitration can perfectly be combined (in med-arb proceedings) by which parties shall first submit their dispute to mediation, in the failure of which the dispute shall then be submitted to arbitration.[87]

From this perspective, the advantages of having specialized mediators that are identified in the EU Online Intermediation Regulation[88] would also fully and similarly apply to specialized arbitrators and arbitration institutions. The EU Online Intermediation Regulation could thus have reflected this and could further have exposed the interactions that can exist between the different dispute resolution mechanisms. By way of illustration, it would be of value to clarify whether a

---

[87] *See e.g.*, the standard WIPO mediation – arbitration clause, Future Disputes: WIPO Mediation Followed, in the Absence of a Settlement, by [Expedited] Arbitration Clause, WIPO *available at* http://www.wipo.int/amc/en/clauses/med_arb/ (last visited Nov. 10, 2019).

[88] EU Online Intermediation Regulation, *supra* note 60, Recital 43 ("[t]he involvement of mediators having specialist knowledge of online intermediation services as well as of the specific industry sectors within which those services are provided should add to the confidence both parties have in the mediation process and should increase the likelihood of that process leading to a swift, just and satisfactory outcome.").

mediation procedure could be initiated without first having to go through the internal complaint-handling system. It would seem appropriate to first go through the internal complaint-handling system and obtain a decision from the provider before initiating mediation proceedings (multi-tier / escalation system).[89]

III. LESSONS

What lessons can we learn from these various European legal developments? First, they show that data disputes will likely be on the rise. These various regulatory instruments and initiatives create rights and obligations relating to personal and non-personal data (such as, by way of example, the right to data portability) that are likely to generate disputes.

Second, these instruments demonstrate that these data disputes are legally quite complex in terms of substantive legal issues not only because they frequently require the taking into account of the interests of third parties[90] but also because they regularly have to balance competing rights and interests in a transversal manner. This can for instance be illustrated by reference to the hypothetical case of the bankruptcy of the provider of data storing or processing services. The EU Non-Personal Data Regulation provides with respect to the portability of non-personal data that the codes of conduct shall provide information before a contract for data storage and processing is concluded covering (among other elements) "the guarantees for accessing data in the case of the bankruptcy of the service provider".[91] This shows the complexity of the legal issues which are at stake because the information and "the guarantees for accessing data" that shall be contained in the codes of conduct are unlikely to offer a full protection in case of bankruptcy of the provider given that the such protection will also depend on the bankruptcy regime that shall be applicable (in the country where the provider is based / where the relevant activity takes place).

Third, and this is the most important point, these regulatory instruments show the importance of establishing appropriate dispute resolution mechanisms for solving these cross-border data disputes. They also evidence the need to conceptualize dispute resolution tools that shall be adapted to address the challenges of massive data disputes that are likely to arise in the (near) future. It is indeed predictable that data disputes and more generally disputes with or connected to

---

[89] This does not seem to be required by Article 12(1) of the EU Online Intermediation Regulation which provides that (Providers of online intermediation services shall identify in their terms and conditions two or more mediators with which they are willing to engage to attempt to reach an agreement with business users on the settlement, out of court, of any disputes between the provider and the business user arising in relation to the provision of the online intermediation services concerned, including complaints that could not be resolved by means of the internal complaint-handling system referred to in Article 11.)

[90] Such as with respect to the right to data portability on the basis of third-party rights and interests in GDPR, *supra* note 2, art. 20(4).

[91] EU Non-Personal Data Regulation, *supra* note 14, Recital 31.

online platforms will grow significantly.[92] Time is thus ripe to develop dispute resolution mechanisms that shall be adapted to address the challenges of digital data disputes and specifically the challenges of what I have called "Massive Online Micro Justice (MOMJ)".[93] This requires the adoption of a concerted approach offering a coherent framework applicable to the different types of disputes and uniform dispute resolution mechanisms for the benefit of all stakeholders. From this perspective, it is not optimal that the various policy instruments that are developed in Europe do not seem to be sufficiently coordinated together in order to provide a global data dispute resolution ecosystem that could apply to the different types of disputes. By way of illustration, it would be most desirable to adopt a uniform approach for the enforcement of the right to data portability that could cover both personal data and non-personal data even if the data are governed by different regulatory instruments. If an individual (i.e. a data subject) faces challenges in the exercise of his/her right to data portability and if the data at issue (it will most likely be frequent) cover both personal and non-personal data (in so-called mixed datasets), it would be valuable to have one single dispute resolution mechanism that shall empower the claimant (data subject) to enforce his / her right efficiently in one single proceeding. The EU institutions will consequently have to ensure the coordination between the regulatory regimes respectively applicable to personal and non-personal data knowing that in practice most data sets will be composed of both personal and non-personal data (mixed datasets).[94]

In this context, mediation and arbitration or other types of alternative dispute resolution methods (similarly to the UDRP) can be very useful mechanisms for settling these (cross-border) data disputes. It may even be risky and counter-productive if the claimant had to use separate dispute resolution mechanisms that would be cost-ineffective and could even lead to potentially conflicting decisions.[95] It would also be worth considering to develop innovative dispute resolution

---

[92] A single judicial decision can generate a massive amount of disputes, as this was the case of the CJEU decision in the "right to be forgotten case" (judgment of the CJEU of May 13, 2014, Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González), which has generated several hundred thousand requests made to Google, *see* https://transparencyreport.google.com/eu-privacy?hl=en (Google has received 852,866 requests to delist since then - status on Oct. 14, 2019).

[93] See Jacques de Werra, *ADR in Cyberspace: The Need to Adopt Global Alternative Dispute Resolution Mechanisms for Addressing the Challenges of Massive Online Micro-Justice*, SWISS REV. OF INT'L & EUROPEAN L. 289, 306 (2016), *available at* https://papers. ssrn. com/sol3/papers.cfm?abstract_id=2783213.

[94] *See* the discussion at footnotes 33 – 38 above.

[95] The right to data portability (for personal data) could be enforced in one proceeding and could not be enforced in another proceeding (for non-personal data) in spite of the hypothetically very close connection between the two categories of data (also because it can be difficult to assess in certain circumstances whether certain data may qualify as personal data under the GDPR).

mechanisms adapted to the digital age that could help avoid/quickly solve digital data disputes, potentially by creating a digital data ombudsman.[96]

In terms of the level of specialization and of expertise of the dispute resolution providers, it would be adequate that such expertise of mediators / experts / neutrals shall also be transversal and shall thus cover issues relating to the portability of all kinds of data, irrespective of whether they are personal data or non-personal data.

In short, it is necessary to avoid the creation of a fragmented, piece-meal dispute resolution system under which each regulatory instrument would provide for its own separate set of dispute resolution rules and principles for data disputes, without consideration of parallel initiatives resulting from other regulatory instruments. The risk of fragmentation does not exist only in case of divergences at the level of substantive law. Fragmentation risks can also arise when dealing with procedural issues. This means that a harmonization at the level of substantive law should be conducted hand in hand with measures of harmonization in terms of procedural / dispute resolution legal principles in order to avoid or at least minimize the risk of fragmentation. This harmonization should obviously and ideally not be limited to Europe but should rather be global knowing the worldwide reach of online activities and the global mobility of data.

What we thus (ideally) need is a new global data dispute resolution ecosystem that shall offer to all stakeholders a multi-tier dispute resolution mechanism for solving data disputes in a fair, equitable and (time and cost) efficient manner.[97] This system should include a transparent internal review process. It should also include mediation and other alternative dispute resolution mechanisms (potentially arbitration - at least in B2B disputes -) that could be selected by the parties. It shall further keep traditional court proceedings before national courts available to the extent this shall be required in order to preserve the right to access to justice of the stakeholders, knowing that court proceedings will most likely be and remain quite burdensome, expensive and lengthy in many instances.

---

[96] By way of example, India has recently created a digital ombudsman for digital transactions, *see* the dedicated page of the Ombudsman Scheme for Digital Transactions, 2019, Reserve Bank of India, *available at* https://www.rbi.org.in/scripts/Bs_view content.aspx?Id=3631; for a recent report on ombusdman schemes, *see* Julinda Beqiraj, Sabina Garahan & Kelly Shuttleworth, *Ombudsman schemes and effective access to justice: A study of international practices and trends*, INTERNATIONAL BAR ASSOCIATION, October 2018, *available at* https://www.ibanet.org/Document/Default.aspx?DocumentUid=77cc70 e5-4cb4-40ae-a11b-4a17d96cfc93; *see* also the recent collection of essays published in the RESEARCH HANDBOOK ON THE OMBUDSMAN (Marc Hertogh, Richard Kirkham eds., Edward Elgar 2018).

[97] It is therefore critical to pursue the development of policy proposals for this purpose, such as the Geneva Internet Dispute Resolution Policies 1.0 project led at the University of Geneva, *available at* www.geneva-internet-disputes.ch.