The legal framework of data subject representation

Andreea Șerban [1*]

[1]Faculty of Law, Alexandru Ioan Cuza University of Iasi, Romania

Abstract. The GDPR provided for new rules on the right of the data subjects to an effective judicial remedy against a controller or a processor where they consider that their rights have been infringed under the Regulation as a result of the processing of personal data. Art. 80 of the GDPR, on the representation of data subjects, is intended to favour private enforcement of EU data protection law, providing for the representation of data subjects by a body or entity which must meet specific requirements in order to exercise the rights conferred to the data subject regarding an effective judicial remedy. The representation of data subjects by a third party in legal actions is possible in two cases: on the one hand, the situation where a data subject mandates the body or organization to represent them or, on the other side, when a body or organization, has the right to lodge a complaint and exercise the rights to effective judicial remedies provided by the GDPR independently of a mandate. This paper will detail the legal framework of this private enforcement tool and analyse the links between data protection and consumer protection from the perspective of collective redress and representation of the interests of a data subject.

1 Introductory considerations

In its ambitious intent, the General Data Protection Regulation (hereinafter, the GDPR) aims to empower the data subjects to the extent of(re)establishing the balance where their rights to data protection are concerned.

The rapid pace of technological development saw the privacy laws fall far behind their times, as legislators needed to catch up with the ever-accelerating digital revolution. At the European level, standing firm for over 15 years as the central legal instrument of the European Union (EU) in this field was Directive 95/46/EC. However, almost two decades later, the Directive barely scratched the surface. Despite its valid and sound legal principles, the Directive has become outdated and insufficient to meet the needs and demands of the

* Corresponding author: andreeaserban20@yahoo.com

21st-century digital environment, with enforcement becoming increasingly challenging given the rapidly evolving technological and digital realities.

The aim of the GDPR has been, since the time of its legislative proposal, the protection of the data subject against unlawful data processing by a controller or a processor [1]. Advocate General Sánchez-Bordona, in his latest opinion on case C-300/21 [2], stated that 'the GDPR does not seek to increase the control of individuals over information concerning them, by merely giving way to their preferences, but rather reconcile each person's right to protection of personal data with the interests of third parties and society'.

The GDPR represents the beginning of European data protection and its framework for privacy reform. The EU has since proceeded to build on the concept of privacy, proposing additional legislation meant either to complement, clarify or apply to more specific situations the basic principles first dignified by the GDPR. The latest examples of the EU's very own 'digital revolution' are key pieces of legislation destined to revamp the European digital legal framework and the sectors that rely on it today, such as the Digital Services Act (Regulation (EU) 2022/2065 of 19 October 2022), Digital Markets Act (Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022), Data Governance Act (Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022), and Data Act [3].

The key aspect of the coming of age of EU privacy laws was the dawn of private enforcement made possible in the wake of GDPR. Soon after the enforcement date of the GDPR, NOYB (None of Your Business, Austria) filed the 101 'dalmatians' complaints [4] against controllers from EU member states on Google Analytics and Facebook Connect integrations. The complaints were filed with the national data protection authorities (hereinafter, DPAs) from Austria, France, Spain, and others, as the criteria for determining the competent filing authority being either the establishment of the controller or the residence of the data subject. The complaints were filed following article 80 (1) of the GDPR. More recently, the Court of Justice of the European Union (CJEU) ruled in judgment C-319/20 *Meta Platforms Ireland Limited* [5] on this precise matter focusing on the article80 of the GDPR and looking at the link between the legal remedies for data protection, commercial practices, and consumer protection law. With the GDPR providing a solid legal basis for the triggering of a growing number of litigations regarding the infringement of the right to data protection, it is worth taking a closer look at the EU rules that govern data protection enforcement, especially the provision enshrined in article 80 of the GDPR, focusing on the representation of the data subject.

The line between data protection and consumer protection is relatively thin. It becomes increasingly blurred in the digital age as it becomes ever more challenging to tell apart "users" and 'consumers'. An individual in the capacity of a data subject should have the right to redress under the rules provided by the GDPR; an individual in the ability as a consumer will have the right to redress under the consumer protection acquis [6]. In a business-to-consumer relationship, a data subject that is also a consumer may exercise their rights twice in both capacities [6].

This paper aims to take a closer look at the data subject representation, analysing the remedies provided by the GDPR and the specific circumstances where article 80 is applicable. Our primary research questions regard the definition of data subject representation, the parties involved in the representation of the data subject, the mandate, the purpose, and the impact of this legal tool.

2 GDPR remedies

The purpose of the GDPR is to empower the data subjects and to arm them with the necessary tools to confront the potential infringements of their data protection rights: where the

controller and/or the processor fail to comply with the rules regarding the right to data protection or the rights derived from the GDPR [7], the data subject can address the competent authority, which is determined by the chosen legal remedy. Thus, the GDPR provides two ways of remedies in articles 77-82: the administrative and the judicial path. The judicial path can occur independently or simultaneously with the administrative way [8], following the application of administrative remedies.

According to article 77 of the GDPR, the data subject has the right to lodge a complaint with a supervisory authority. Where a controller and/or a processor has infringed any of the rights of the data subject regarding their data, it is recommended that the data subject first exercise their rights by contacting the competent controller and/or processor, as it is relevant to have a clearer view of how the data is being dealt with and how the data subject's rights have been infringed [9]. Yet, such a step is not compulsory as the GDPR does not provide for it. While a lack of answers or resolution on behalf of the controller/processor might provide additional support for a legal claim in the respective case, the data subject has the power to address their case directly to the data protection authority. It must be noted that some authorities require data subjects to provide supporting evidence. For example, correspondence with the controller, contracts, or screenshots could be *supporting evidence*. Nonetheless, it is possible to lodge the complaint without such supporting evidence.

There is a divide between DPAs concerning the requirements that complaints must observe, as well as the necessity for prior documented correspondence between the data subject and the controller: data subjects are encouraged to first bring the data protection issue to the attention of the relevant controller, or they receive an indication in the complaint form to do so, without being made clear to them whether it is a mandatory condition or not.

For example, the Hamburg Data Protection Authority recommends that the data subject first contact the data controller as there frequently is a data protection officer who provides independent consultancy regarding the protection of data – this step may occasionally prove itself to be a faster way to find a solution fit for the interests of the data subject [10]. On the other side, the Irish Data Protection Commissioner, in its contact form, only allows the finalization and submission of the complaint form provided if the data controller has been priorly contacted, inviting this way the data subject to first raise their concerns with the data controller [11]. In the latter case, the data subject may only contact the DPA following a previous inquiry with the respective data controller and only after receiving a negative reply to their claim. – *e.g.,* the data subject requests a data controller to delete their data, and the controller refuses. Per the Decision of the Romanian Data Protection Authority, no. 133/2018, regarding the procedure for receiving and handling complaints, according to article 5(1), when lodging a complaint, it is mandatory to specify the subject matter of the complaint in detail, as well as the steps taken by the complainant concerning the controller and/or controller targeted by the complaint or, where is the case, the information available to support the allegations, and to attach the conclusive evidence, where available.

The judicial path is multiforme. It must be noted that this path can be taken following a decision of the supervisory authority or directly against the controller or processor, thus independently and without prior informing or addressing the data protection authority. The GDPR further details the judicial instruments that the data subjects have at their disposal: article 78 details that the data subject has the right to an effective judicial remedy against a supervisory authority, and article 79 establishes an effective judicial remedy of the data subject against a controller or processor.

These provisions enshrine the EU legal framework for effective judicial remedies in data protection, while the procedural rules remain a competence of each Member State. The Romanian Data Protection Authority stated in its Decision no. 133/2018, art. 5(2), that if the complainant has lodged a complaint with a national court with the same subject matter and against the same controller or processor, the data subject must bring the complaint to the

attention of DPA. Art. 8(2) of this Decision further states that the Romanian Data Protection Authority may close or suspend the complaint where a similar complaint was lodged with a national court, while art. 8(3) states that the competent court is the one from the establishment of the controller or processor or the habitual residence of the data subject.

Article 79 of the GDPR has a broader application than article 78. The obligation foreseen in article 78 to provide an effective judicial remedy against a legally binding decision of the DPAs does not guarantee an effective judicial remedy" in itself. There are claims that cannot fall under the remit of the DPA [12].

As the right to data protection is not new, nor is the GDPR a legal innovation anymore, it is now litigation that steals the spotlights: over the past years at the EU level, the attention of the data subject to data protection issues has intensified due to the rise of cases at the CJEU. With jurisprudence highlighting growing loopholes and showcasing the rigid incapacity to adapt to current times - thinking of *Google Spain* [13] or *Schrems* [14] cases - new calls for improving the European legislation are made for supporting the role of the data subjects and the underlying the importance of providing alternative courses of action to promoting adequate protection [15].

However, there is a fundamental problem of affordability and accessibility of legal counsel and the legal capacity for data subjects to engage in litigation to defend their rights effectively. The lack of understanding of data protection matters or financial or legal support for the act in situations where data protection rights are infringed might prove to be one bridge too far for the average data subject. Therefore, the GDPR, unlike its predecessor, Directive 95/46/CE, provides for new legal instruments regarding data subject representation, ultimately drawing inspiration from the consumer protection law.

3 Collective redress in data protection matters

Before diving into the data subject representation and collective redress in data protection matters, it is worth considering the legal notion of collective redress and defining the terminology in both the data protection and the consumer protection context.

Initially created as an instrument to avoid repetitive litigation in 17th-century England, collective redress has evolved since its Elizabethan days to become a much more modern tool. The mechanisms for collective redress and class action are developing rapidly at the global level due to multiple reasons: on the one side, there is a shifting attitude toward favouring these types of collective claims; on the other side, the rights of individuals have expanded in many areas together with the number of civil society organisations with resources to take such initiatives on, allowing litigants being more interested and aware about their rights nowadays [16] – a clear example of how the data protection rights provided the foundation for an increasing number of litigation cases.

In short, a 'class action is a legal procedure which enables the claims (or part of the claims) of a number of persons against the same defendant to be determined in the one suit' [17]. The complex nature of this procedural instrument has been the subject of controversy over time, having been described either as a 'Frankenstein monster' or 'one of the most significant procedural developments of the century' [17].

Collective redress refers to any legal mechanism that provides a possibility to collectively claim cessation or prevention of unlawful business behaviour or collectively demand compensation in mass harm situations when two or more natural or legal person claim to have suffered damage resulting from the same illegal activity. Harm could be material or immaterial – the latter being the case with privacy and data breaches.

Over the past years, class action cases concerning data protection and privacy before the Courts in the United States and the United Kingdom have been rising steadily. In the US, LinkedIn had to make settlements on weak password security and the scanning of its users'

contact lists [18]. In the UK, a class action was filed against a supermarket chain over mass personal data theft [19].

The collective redress mechanism has been developing in a fragmented fashion in the European Union, both at the national and the EU level, as well as sector-wise. In the Commission Recommendation of 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law [20], collective redress is defined as '(i) a legal mechanism that ensures a possibility to claim cessation of illegal behaviour collectively by two or more natural or legal persons or by an entity entitled to bring a representative action (injunctive collective redress); (ii) a legal mechanism that ensures a possibility to claim compensation collectively by two or more natural or legal persons claiming to have been harmed in a mass harm situation or by an entity entitled to bring a representative action (compensatory collective redress).'

The Recommendation further defines representative action as "an action which is brought by a representative entity, an ad hoc certified entity or a public authority on behalf and in the name of two or more natural or legal persons who claim to be exposed to the risk of suffering harm or to have been harmed in a mass harm situation whereas those persons are not parties to the proceedings".

Collective redress was under the spotlight before the CJEU. In the *Maximilian Schrems v Facebook Ireland Limited* [21] case, the questions regarding the role of class action within the legal framework of the EU further developed the discussion, with broad implications for data protection and consumer rights alike [22]. Two issues were of relevance for the data protection representation matter: (1) on the one side, the activities of Max Schrems in data protection and privacy matters and the fact of being assigned the claims of numerous consumers for the purpose of law enforcement entailed the loss of his private status as a consumer within the meaning of the Regulation on judgments in civil and commercial matters. The Court concluded that while the concept of the consumer must be strictly construed, excluding the activities of Schrems would prevent an effective defence of consumer rights and thus, as per point 41 of the Court decision, "the activities of publishing books, lecturing, operating websites, fundraising and being assigned the claims of numerous consumers for the purpose of their enforcement do not entail the loss of a private Facebook account user's status as a 'consumer' as understood within the meaning of art. 15 of Regulation (EU) 44/2001; (2) on the other side, the Court was asked if a consumer could assert in the courts of the place where they have domiciled not only their own claims but also the claims assigned to them by other consumers, possibly domiciled in the same Member State, other Member State, or in 3rd countries. The Court concluded that the fact that consumers could bring proceedings where they are domiciled 'does not entail the jurisdiction of this court for similar claims assigned to the consumer' [23]. This means that, in this case, Schrems could enforce his claims before the court relevant according to his domicile, but not the claims of other consumers.

While it represents a milestone for the evolution of consumer rights enforcement, the judgment underlines the law's current state through the Court's refusal to create a new consumer forum – the current legislation does not yet support trans-border consumer actions [23]. The European Consumer Organisation (BEUC) noted that 'with this judgment, the European Court of Justice has made expectations collapse that consumers can join forces in one court to achieve redress in mass harm claims.' [24] BEUC also noted that this judgment was a call to action for the EU for a collective redress tool to shift the balance in favour of the consumer and produce effects at the European level.

Looking back at the state of the collective redress legislation in Member States across the EU before 2018, we can observe discrepancies and significant differences between Member States [25]: while some countries did not provide any type of collective actions for damages,

others provided within their framework very complex procedures that rendered the collective redress mechanism highly expensive, burdensome and inaccessible for consumers in different matters, let alone consumers as data subjects in data protection matters.

The Austrian Constitutional Court accepted the admissibility of the joint individual applications in the constitutional action brought by Mr. Tschohl with 11128 other applicants on the compatibility between the Federal Constitutional Law and the transposing the directive on Data Retention into Austrian Law. The action served as the origin of the request for a preliminary ruling in Case C-594/12 before the CJEU [26].

In *Fashion ID* [27], it was asked whether the Data Protection Directive precluded national legislation from granting standing to consumer protection associations to bring actions against infringers of data protection laws. The Court interpreted the provisions of art. 22-24 of Directive 95/46 as 'not precluding national legislation which allows consumer-protection associations to bring or defend legal proceedings against a person allegedly responsible for an infringement of the protection of personal data.' The Court noted that article 80(2) of GDPR reflects the intention of the European legislation by expressly authorizing 'the bringing of legal proceedings by such an association', confirming that Directive 95/46 did not preclude such an action [27].

3.1 Collective actions according to GDPR

One of the novelties of the GDPR was the provision for collective redress in art. 80. Per art. 80 (1) of the GDPR, 'The data subject shall have the right to mandate a not-for-profit body, organization or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.' Art. 80 (2) of the GDPR provides that 'Member States may provide that anybody, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.'

For further interpretation of art. 80, GDPR provides recital 142. While not a binding provision, recital 142 reiterates the right of the data subject 'to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State […]'. Additionally, recital 142 provides that 'body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject mandate'.

Other related provisions can be found in the EU's Law Enforcement Directive 2016/680, respectively in art. 55 – representation of data subjects, art. 52 – right to lodge a complaint with a supervisory authority, art. 53 – right to an effective judicial remedy against a supervisory authority, and art. 54 – right to an effective judicial remedy against a controller or processor.

Why was this article needed in the GDPR? In a report of the European Union Agency for Fundamental Rights (FRA) on access to data protection remedies in EU Member States [28], addressing the protection of personal data as enunciated by art. 8 and the right to an effective remedy as provided for by art. 47 of the Charter, it was shown that broadening collective action in data protection matters was relevant for increasing accessibility and efficiency of the remedies in the data protection area [28]. Intermediaries and legal professionals interviewed for the report from most of the EU Member States have suggested a class action

type of procedure, arguing that these 'are related to the correction of power relations in the proceedings and possible reduction of costs for the individuals subjected to the data protection violations'. In the absence of such procedures, such affordability and accessibility issues, among others, represent veritable barriers that are significantly off-putting in certain sensitive sectors, in particular small commerce and individual consumers. Thus, in the data protection field, a collective redress mechanism is a valuable tool concerning the number of potentially affected people, reducing significant individual costs, promoting accessibility, and creating a more efficient procedure for effectively protecting rights. The European Commission, in its Recommendation [29], recital 7, states that 'amongst those areas where the supplementary private enforcement of rights granted under Union law in the form of collective redress is of value, are consumer protection, competition, environment protection, protection of personal data, financial services legislation and investor protection.'

Art. 80 GDPR is a novelty in data protection, having no equivalent in Directive 95/46, Convention 108, or Modernised Convention 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data). As the previous legal framework for data protection was based on a directive, Member States had the competence to transpose these provisions into their national legislation and thus determine how they would work in practice, ultimately resulting in different national approaches across the EU Member States.

The title of art. 80 GDPR regards the 'representation' of data subjects, with this provision establishing 'a number of rights or modalities of a single right, and foreseeing the possibility, at national level, of others' [12].

Looking at its first paragraph, it should be noted that data subjects can mandate bodies, organizations, or associations that comply with the following requirements: (1) not-for-profit – e.g., the organization is not constituted for commercial gain, its purposes are to benefit the public; (2) properly constituted per national legislation; (3) has statutory objectives in the public interest - e.g., a precondition for allowing Member States to provide for the possibilities of these entities to act without an individual mandate [12]; (4) to act in the field of data protection – e.g., the activities of the entity should concern the promotion of data protection rights and freedoms.

The qualifying criteria have been subjected to criticism in recent literature, having been considered limitative, in practice posing more questions than answers [22], as the aim of these criteria 'can be inferred' in national legislations of some Member States.

The mandate that article 80(1) GDPR refers to concerns the right of the data subject to mandate any of the entities that cumulatively meets the criteria to lodge the complaint on his or her behalf and to exercise the rights referred to in articles 77-79, and the right to receive compensation referred to in article 82 […] where provided for by Member State law.

This first form of class action provided for in art. 80(1) is similar to the opt-in class action as understood in common law [30]. It is conditioned by a manifestation of will that results in the mandate given by the data subject or data subjects to an entity established per the criteria mentioned above. Where more data subjects express their will in this sense, the mandate is common for all of them, and the mandated entity will commonly represent them.

As a rule, all data subjects can mandate. In practice, though, this will depend on the existence of entities properly established according to the legislation of a Member State that could exercise the data subject's right of representation as foreseen by art. 80(1) GDPR. The existence of the mandate determines a choice of forum restriction by the jurisdictional provisions relevant to the content of the mandate [12].

As for the last part of the 1st paragraph of art. 80 GDPR, the right to receive compensation as provided by art. 82 GDPR, the intention of the legislator is clearly to leave to the legislative framework of each Member State to provide for compensation rules concerning data protection matters. In the sense of the line to exercise the right to receive compensation

referred to in Article 82 on his or her behalf where provided for by Member State law, the exercise of this right is not established as a rule but rather as a possibility that is provided only in the case of this type of class action. As we will see in art. 80(2), the same possibility is not provided for the opt-out type of class action.

Looking at the wording of art. 82 GDPR, we note that this provision leaves no room for interpretation or discretion in its implementation by the Member States. The article, titled right to compensation and liability, has a direct effect regardless of its implementation in the respective national legal orders [12].

Yet, concerning the mandate for representation given to an entity, as established in art. 80(1) GDPR, the right to compensation has a differentiated approach, which differs depending on the national legislative framework of each Member State.

As mentioned above, a closer look at art. 80(2) GDPR reveals an opt-out form of class action [30]. An entity established under the criteria set out in this paragraph may lodge a complaint, independently of a data subject's mandate, with the data protection authority and/or exercise the rights provided by articles 78-79 GDPR.

Regarding this paragraph, we note that it is not an obligation or a rule to be followed but rather an option that the Member States can further provide for in their national legislation.

As for the entities subject to this provision, they can refer to anybody, organisation, or association, as mentioned in paragraph (1). Therefore, those properly established and respecting the criteria abovementioned. These entities do not act on behalf of a data subject or with a mandate. At the same time, their interest in acting must not be manifested in abstracto or as a theoretical public interest concern. The entities may act only if they consider that the rights of a data subject […] have been infringed as a result of the processing. Thus, the entities may even represent an unidentified yet presumably affected data subject [12].

Compared to the 1st paragraph, this provision raises questions regarding the forum. The entity may bring the complaint to the competent data protection authority as provided by art. 77 GDPR, yet not having an identified data subject could mean that the possibility of predicting the possible forum is considerably decreased. Thus, the competent data protection authority can also be the one in the Member State where the alleged infringement took place. In Weltimmo [31], the Court decided that the Hungarian DPA was competent to hear the claims against a Slovakian company that targeted its data processing in Hungary and affected data subjects from Hungary.

Deconstructing art. 80 GDPR, we see that, in practice, its application might lead to the increased involvement of consumer protection associations and, as noted by Gierschmann [32], increased pressure on controllers/processors to reach compliance, as well as a rise in the number of complaints that have their legal basis on this art.

Also, concerning the application of paragraph 2 of art. 80 GDPR, it depends on the will of each Member State to provide a rule that ensures the application of this form of class action, as well as the interest and devotion of entities to pursue such actions without a mandate.

3.2 Brief considerations on Directive 2020/1828 on representative actions for the protection of the collective interests of consumers and its connection to GDPR

With the Representative Actions Directive (Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 – 'RAD'), a new era of European class actions began.

In 2017, *the European Commission announced a new deal for consumers* in the aftermath of the Dieselgate scandal [33]. This new deal also included the proposal for the directive on representative actions that was later adopted in 2020.

This new instrument is the result of a legislative evolution at the EU level in response to the issue of limited resources of representative entities that prevented the initiation of mass claims [34].

In brief, RAD requires Member States to adopt at least one efficient collective action mechanism that aims to enable entities to bring representative actions against traders concerning infringements of EU law in matters such as data protection, product liability, telecommunications, financial services, etc [35].

RAD grants standing to *qualified entities*. These are being defined in art. 3(4) RAD as 'any organisation or public body representing consumers' interests which has been designated by a Member State as qualified to bring representative actions'. Art. 4(3) RAD further states the criteria to be met for the qualified entities: (a) *legal person* – constituted in accordance with the national law and *can demonstrate 12 months of actual public activity in the protection of consumer interests prior to its request for designation*; (b) *statutory purpose* that demonstrates the entity's *legitimate interest in protecting consumer interests*; (c) non-for-profit character; (d) not subject of insolvency proceedings and not declared insolvent; (e) *independent and not influenced by persons other than the consumers*; (f) ensures transparency – making publicly available information that demonstrates the compliance to the criteria as mentioned above.

RAD also lays down the redress measures defined in art. 3(10) as measures that 'require a trader to provide consumers concerned with remedies such as compensation, repair, replacement, price reduction, contract termination or reimbursement of the price paid, as appropriate and as available under Union or national law'.

At first sight, the interplay between the GDPR and RAD is a complicated relation up for interpretation. On the one side, art. 80 GDPR establishes an exclusive framework, and all representative actions must necessarily respect its requirements. Thus, should there be no mandate, as art. 80(2) does not provide for it, representative entities cannot request compensation. Therefore, art. 80 GDPR would always apply, while RAD provisions would be seen as devalued in data protection matters [36]. On the other side, another question that might raise concerns is the possible parallel litigation channels. In this case, actions that do not fall within the scope of art. 80(2) GDPR could be pursued under national law following its transposition of the provisions of RAD. Therefore, the issue stands in the fact that RAD appears to impose even stricter conditions than GDPR [36].

3.3 Brief considerations on CJEU C-319/20 Meta Platforms Ireland Limited

The European discussion around class actions in data protection matters significantly increased with the Judgement in the C-319/20 *Meta Platforms Ireland Limited* case before the CJEU. The Federal Union of Consumer Organizations and Associations (Verbraucherzentrale Bundesverband - vzbv) brought an action for an injunction before the Regional Court in Berlin, Germany, against Meta Platforms Ireland for the infringement of rules concerning certain users' data. The action was brought *independently of a specific infringement of a data subject's right to protection of his or her data and without being mandated to do so by such a person* [5]. The action reached the Bundesgerichtshof, the German Federal Court of Justice, which voiced its doubts concerning the admissibility of a consumer group bringing a claim on behalf of a group of users, questioning whether German national law provisions which allowed for consumer protection associations to bring these claims were indeed compatible with the GDPR [5].

The question referred to the Bundesgerichtshof regarded whether the provisions of arts. 80 and 84 GDPR precluded the national rules which empower competitors, associations, entities, and chambers entitled under national law to bring actions independently of an infringement of specific rights of data subjects and without a mandate from a data subject [5].

The Court confirmed that art. 80(2) GDPR is not '*precluding national legislation which allows a consumer protection association to bring legal proceedings, in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of the data subjects, against the person allegedly responsible for an infringement of the laws protecting personal data, on the basis of the infringement of the prohibition of unfair commercial practices, a breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions, where the data processing concerned is liable to affect the rights that identified or identifiable natural persons derive from that regulation'*. [5]

The Court confirmed that vzbv could bring the claim independently of the infringement of specific rights and regardless of a particular mandate from a data subject. The immediate impact of this confirmation is the bringing of a broader protection net for consumers, who can now be offered a more significant number of tools to defend their rights.

4 Concluding remarks

The data protection framework is still a veritable construction site, an ongoing process of construction and reconstruction of an evolving framework in a revolutionary world. The class action mechanism is only one representation of this constant evolution, a necessary tool now reinvented to keep up with the pace of the digital world, ensuring that the protection of rights is effective and does not leave out those most vulnerable.

The provisions of the Representative Actions Directive confirmed and doubled down by the most recent jurisprudence, together with the GDPR provisions for redress, stand to create a solid basis for private enforcement, promoting increased levels of litigation from consumer groups, thus keeping pressuring controllers and processors accountable and providing the right incentives for these entities to focus even more on adequate compliance.

Nonetheless, even with an improved and updated legal framework, it is still very much up for discussion how the provisions of art. 80 GDPR will be ultimately implemented, given that there is still enough room for interpretation and for Member States to choose the option to (not) legislate in this matter.

References

1. D. Hallinan, EDPL, **5 (3)**, 293–99, DOI: 10.21552/edpl/2019/3/5 (2019)
2. Court of Justice of the European Union, Opinion of the Advocate General Campos Sánchez-Bordona delivered on 6.10.2022, C-300/21, *UI v Österreichische Post AG* (2022)
3. Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final (2022)
4. EU-US Transfers Complaint Overview, URL: https://noyb.eu/en/eu-us-transfers-complaint-overview, accessed 10.01.2023
5. Court of Justice of the European Union, Judgment of 28.04.2022, Case C-319/20, *Meta Platforms Ireland Limited*
6. M.R. Leiser, *Dark patterns': The case of regulatory pluralism between the European Union's consumer and data protection regimes*, in E. Kosta, R.Leenes, I. Kamara (eds.), *Research Handbook on Eu Data Protection Law*, Research Handbooks in European Law, 265 (Edward Elgar Publishing, United Kingdom, 2022)
7. A. Serban, Analele Științifice UAIC, SSJ, **64**, 167 (2018)

8. C.T. Ungureanu, Revista „Dreptul", **10**, 85 (2018)
9. *Exercise Your Rights – Article 77 – complain to your DPA*, URL: https://noyb.eu/en/exercise-your-rights-article-77-complain-your-dpa, accessed 10.01.2023
10. *Elektronische Beschwerde*, URL: https://datenschutz-hamburg.de/beschwerde/, accessed 20.10.2022
11. *Data Protection Commission – Contact Us*, URL: https://forms.dataprotection.ie/contact, accessed 20.10.2022
12. C. Kuner, L. A. Bygrave, C. A. Docksey. Commentary on the EU General Data Protection Regulation, 1135 (Oxford University Press, 2018)
13. Court of Justice of the European Union, Judgement of 13.05.2014, Case C-131/12, *Google Spain* (2014)
14. Court of Justice of the European Union, Judgement of 06.10.2015, Case C-362/14, *Maximillian Schrems V Data Protection Commissioner* (2015)
15. P. Hustinx, *The role of Data Protection Authorities*, in S. Gutwirth, Y. Poullet, P. De Hert, C.De Terwangne, S. Nouwt (eds.), Reinventing data protection?, 136, 137 (Springer Science & Business Media, 2009)
16. *Collective redress class actions 2021*, URL: https://practiceguides.chambers.com/practice-guides/collective-redress-class-actions-2021, accessed 20.10.2022
17. R. Mulheron, C. Baudenbacher, P.Tresselt, T.Orlygsson*, The class action in common law legal systems: a comparative perspective,* 3 (Bloomsbury Publishing, London, 2004)
18. J. Roman, *LinkedIn Settles Data Breach Lawsuit*, URL: https://www.bankinfosecurity.com/linkedin-a-7229, accessed 23.10.2022
19. *English High Court Finds Supermarket Liable for Data Breach by Employee in First Successful Privacy Class Action*, URL: https://www.insideprivacy.com/data-security/english-high-court-finds-supermarket-liable-for-data-breach-by-employee-in-first-successful-privacy-class-action/, accessed 23.10.2022
20. Commission Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law, OJ L 201 (2013)
21. Court of Justice of the European Union, Judgement of 25.01.2018, C-498/16, *Maximilian Schrems v Facebook Ireland Limited* (2018)
22. L. Jančiūtė, International Data Privacy Law, **9 (1)**, 3 (2019)
23. J. Haslach, Common Market Law Review, **56, Issue 2**, 570 (2019)
24. *EU top court ruling exposes need for European collective redress tool*, published on January 25, 2018, URL: https://www.beuc.eu/press-releases/eu-top-court-ruling-exposes-need-european-collective-redress-tool, accessed 23.10.2022
25. BEUC, *Where does collective redress for individual damages exist?*, Updated in October 2017, BEUC-X-2017-117
26. Court of Justice of the European Union, Judgment of 08.04.2014, C-293/12 and C-594/12, *Digital Rights Ireland Ltd* (2014)
27. Court of Justice of the European Union, Judgment of 29.07.2019, Case C-40/17, *Fashion ID* (2019)

28. European Union Agency for Fundamental Rights, *Access to data protection remedies in EU Member States* (2013)
29. Commission Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law, OJ L 201 (2013)
30. C.T. Ungureanu, Drept internaţional privat european în raporturi de comerţ internaţional, 154 (Hamangiu, Bucuresti, 2021)
31. Court of Justice of the European Union, Judgment of 01.10.2015, Case C-230/14, *Weltimmo* (2015)
32. Gierschmann *apud* P. Voigt, A. von dem Bussche, The EU General Data Protection Regulation (GDPR), A practical guide, 1st Ed., 216 (Springer International Publishing 10, no. 3152676, 2017)
33. European Commission, *Dieselgate*, URL: https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions/dieselgate_en, accessed: 10.02.2023
34. A. Biard, *Collective redress in the EU: a rainbow behind the clouds?,* in ERA Forum, vol. 19, no. 2, 189-204 (Springer Berlin Heidelberg, 2018)
35. F. Rielaender, ICLQ, **71**, **no. 1**, 108, DOI: 10.1017/S0020589321000403 (2022)
36. A. Pato, *GDPR Collective Litigation Against Facebook*, URL: https://verfassungsblog.de/gdpr-collective-litigation-against-facebook/, accessed 10.02.2023