Collective Data Protection Litigation

A Comparative Analysis of EU Representative Actions and US Class Actions Enforcing Data Protection Rights

Karl Wörle
Lecturer; Head of Business Law Department;
University of Applied Sciences BFI Vienna, Vienna, Austria
karl.woerle@fh-vie.ac.at

Oskar Josef Gstrein* | ORCID: 0000-0003-0546-8684
Associate Professor Human Dignity in the Digital Age;
Programme Director BSc Data Science and Society; Jantina Tammes School Theme Coordinator Data Autonomy;
Campus Fryslân, the Netherlands
*Corresponding author
o.j.gstrein@rug.nl

Received 21 September 2023 | Accepted 18 March 2024 | Published online 24 April 2024

Abstract

At first glance data protection litigation seems to be a niche topic. Yet, record sum compensation such as those resulting from the Meta – Cambridge Analytica lawsuit (725 million USD) reveal enormous practical relevance. This proceeding took the form of a class action, brought before a Californian court. Such collective proceedings might sweep across the Atlantic, as the EU Directive on Representative Actions introduced a new collective litigation mechanism. We commence our comparative analysis by outlining the relevant legal landscapes in the EU and the US, give an account of the latest developments, and examine relevant case law and scientific literature (paras. 1.–4.). Subsequently, the law and economics of data protection litigation are explained (para. 5.), which will serve as standard of comparison. On this basis, in para. 6. the article contrasts the efficiency of collective litigation mechanisms, enabling enforcement against data protection infringements, with the objectives of evaluating the legal status quo and distilling proposals for future legal policy.
Keywords


1 Introduction

Collective proceedings have been commonplace in the United States of America (hereinafter USA or US) for a long time.1 In recent years in continental Europe the Volkswagen emissions scandal (Dieselgate) has drawn public attention to the obstacles consumers face in cases of mass claims, highlighting the shortcomings of individual litigation.2 Traditionally, European collective dispute resolution mechanisms such as joint actions or model actions are rather limited in scope (except for the progressive Dutch wcam-collective settlement regime). To remedy the situation, the Directive on Representative Actions (Directive (EU) 2020/1828; hereinafter rad or Directive) aims to make sure that a minimum legal standard for representative actions is available in all EU Member States, thereby harmonizing the patchwork of existing national collective proceedings.3

The procedural framework of the rad addresses recent developments in the field of consumer protection, in particular regarding an increasingly digitalised marketplace. As consumers struggle to retain control over their data – considered a commodity in informational or surveillance capitalism, as the successor of industrial capitalism4 – one designated area of enforcement of the

---

3 It must be noted that the Directive does not prevent Member States from adopting or retaining in force procedural means for collective proceedings at national level (see Art 1 para 2 rad).
Directive are violations of the General Data Protection Regulation (hereinafter GDPR). Even though the sanction regime of (substantive) administrative fines of the GDPR (Art. 83) is accompanied by a right of data subjects to an effective judicial remedy (Arts. 79, 82 GDPR), individual enforcement has proven to be overly complex and frequently ineffective. In contrast, collective proceedings permit consumers to join forces against internet giants (see in particular para. 5). In this article, we focus on exploring the intersection of two very distinct and complex areas of law, data protection and collective litigation. We aim at highlighting the hurdles of data protection litigation and evaluating how well the RAD remedies the complex enforcement dilemma. We analyse the topic with a comparative and law and economics approach, considering empirical evidence if possible. As collective litigation has a long tradition in the USA, and regarding data privacy litigation, such a comparison promises to be rewarding. As the RAD grants the EU Member States a broad margin of discretion in its implementation, it does not suffice to examine the Directive as such. Hence, it seems necessary to take a closer look at its national transpositions (see para. 3.). The enforcement of data protection law with the RAD – as a procedural mechanism of consumer protection – prompts numerous questions regarding the interrelation between data protection and consumer law, as well as a possible further integration of their respective enforcement systems (see para. 4.). In the detailed analyses (para. 6.) we contrast the efficiency of collective litigation mechanisms, the paragraph being subdivided in several key enforcement questions: At the outset of a representative action admissibility issues arise (para. 6.1) and the legislator must make a choice between an opt-in mechanism of voluntary participation, or an automatic inclusion in an opt-out system (para. 6.2). Damages in collective actions are very complex to calculate, therefore settlements play a pivotal role (para. 6.3). In particular, non-material damages are most difficult to quantify (para. 6.4). A tremendous challenge to collective data protection litigation is the clash with the traditional public authority-model of the GDPR (see para. 6.5.). Finally, we address the critical question if the complementation of the existing sanction regime with the new collective litigation mechanism might lead to over-enforcement (see para. 6.6).

5 Annex I enumerates 66 provisions of Union law to be covered by the Directive (Recital 14 RAD).
2 Collective Proceedings and Legal Culture

The Anglo-American class action model has its origins in medieval group litigation in England, the so-called Bills of peace. They were brought before the English Chancery Courts and originate in equity law. Their concept was soon adopted in the US, where the class action has been codified for the first time in 1833. In 1938 the Federal Rules of Civil Procedure (FCRP) were enacted, with the novelty of binding absent parties. In 1966 the class action was completely overhauled and brought into the shape as it is known today. This reform took place during the civil rights movement and aimed to battle racial segregation and workplace discrimination. Another goal of the reform was to facilitate the enforcement of scattered damages, which made class actions very popular in antitrust and securities actions.

In US class action, the class is represented by the named plaintiff (also referred to as class representative) initiating the claim in their own name and at the same time on behalf of all other harmed individuals. In case the parties reach a class action settlement the court must approve that the settlement agreement is fair, reasonable, and adequate (Rule 23(e) FCRP).

From a meta-perspective, the class action is a manifestation of the common law-typical adversarial system, relying on private individuals motivated by

---

9 D. Hensler et al., *Class Action Dilemmas: Pursuing Public Goals for Private Gain*, (Santa Monica: RAND corporation, 2000) p. 10. Groups of individuals could bring complaints about communal harm, e.g. merchants manipulating the marketplace or church officials disturbing religious peace. The groups were granted a hearing and remedies by government institutions. Over the years, such representative actions for collective harm turned into an individualized justice system.

10 S. Eichholtz, *Die US-amerikanische Class Action und ihre deutschen Funktionsäquivalente* (Tübingen: Mohr Siebeck, 2020) pp. 33. Equity law provides a remedy for situations where the usual court system is not flexible enough to deliver a fair resolution to a case.

11 D. Hensler et al., *Class Action Dilemmas: Pursuing Public Goals for Private Gain*, (Santa Monica: RAND corporation, 2000) pp. 10. There were three different types of class actions (true, hybrid and spurious), while the first two brought the novelty of binding absent parties.


economic self-interest rather than on public officials.\textsuperscript{15} Besides its principal purposes of granting compensation and adjudicating the individual case, private law enforcement also serves a public function: As traders have to fear severe judgements, condemning them to fierce compensation payments, they are deterred from wrongdoing.\textsuperscript{16} Private enforcement thereby becomes a tool to implement public policy and to achieve social goals (regulation through litigation).\textsuperscript{17}

However, the achievement of such noble public interest motives is frustrated by several flaws in the US class action system. US-American attorneys frequently represent clients on basis of contingency fee agreements, where attorneys are promised a percentage of the amount in dispute. Such fee arrangements are prohibited in many countries. Opposed to continental European tort law, courts do not only order the tortfeasors to compensate the damage they have caused. Punitive damages are being added, usually calculated as a multiple of compensatory damages. This can lead to excessive damage awards.\textsuperscript{18}

\begin{itemize}
\end{itemize}
For US-class actions the opt-out-mechanism is characteristic, where harmed individuals automatically become part of the class – which might lead to due process-concerns (see in further detail para. 6.2). Such peculiarities of US class action – among others – result in a toxic cocktail, fostering abuse by slick attorneys. They can bring so-called strike suits of questionable merit with the purpose of gaining a settlement before going to court (“bounty hunting” or “blackmail-settlements”).

In contrast to this Anglo-American approach, continental European countries use an inquisitorial court system. Here the role of the judge is more prominent and active, with less space for private autonomy and party disposition. The policy-leitmotif is public welfare and solidarity, instead of individualism and competition. Hence, there is traditionally less private enforcement, even though European private and procedural law seems to be in a transformation process and shifts in a similar direction as in the US.

3 Genesis of the Representative Actions Directive and National Transpositions

For a long time, class actions have been considered incompatible with the European legal culture. The first step towards harmonisation of collective proceedings in the EU and a more consistent approach to collective redress was achieved by the Injunctions Directive (2009/22/EC). A shortcoming of the Injunctions Directive was – as the name suggests – that it has been
limited to injunctive measures. Hence, it could stop illegal practices, yet consumers could not collectively sue for compensation or repair. In 2018 the EU adopted a so-called “New Deal for Consumers”, by which it modernises and strengthens the enforcement of consumer law. Several measures were enacted including the RAD, replacing the Injunctions Directive. In contrast to its predecessor, the RAD also permits redress measures (e.g. compensation or repair, see Art. 9 RAD). Thereby the RAD aims to achieve a high level of consumer protection (Recital 76 RAD; Art. 1 para. 1 RAD) and to deter unlawful practices (Recital 5 RAD).

The RAD aims to avoid the vices of US-style class action: First, collective redress appears in the EU under a changed label. Instead of class actions we encounter “representative actions”. The initiation of representative actions is primarily in the hands of consumer organizations (qualified entities). As they have to meet strict criteria including non-profit making character (Art. 4 RAD) and funding restrictions to avoid conflicts of interest (Art. 10 RAD), several safeguards are put in place to impede abusive litigation and bounty hunting.

---


27 For the sake of clarification, if we make reference to “injunctive measures” in this paper, measures to cease or prohibit practices are meant and we do not refer to provisional respectively interim measures, as they are colloquially sometimes called “injunctions”. Yet, an injunctive measure could be enforced both as a provisional or as a definitive measure (see Art. 8 RAD), but as said when using the term injunctive in this paper we refer to court orders to cease or prohibit practices.


31 H. Ruschemeier, „Kollektiver Rechtsschutz und strategische Prozessführung gegen Digitalkonzern“, MMR (2021), 942, 944.


Further, to prevent the misuse of representative actions, the awarding of punitive damages should be restricted (Recitals 10 and 42 RAD). Also, the controversial opt-out is not compulsory, but only a Member State option to consider during implementation (Art. 9 para. 2 RAD).35

In line with the principle of procedural autonomy the rad does not regulate every minor aspect of the collective proceeding (Recital 12 rad). Member States are granted a broad margin of discretion on how to transpose the required procedural mechanism for representative actions (Recital 11 rad). Therefore, this article takes a closer look at two national implementations which have the potential for significant practical impact (as outlined below), namely the German and the Dutch transposition.36 Both jurisdictions have vast experience with collective litigation, in Germany due to the Volkswagen emissions scandal and in the Netherlands because of the well-established WCAM collective settlement regime (Wet collectieve afwikkeling massaschade). Further, these jurisdictions are illustrative for collective proceedings in the continental European legal tradition, to draw a comparison with data protection litigation in the US. Unfortunately, the rad has not yet been transposed in Austria, home of data protection pioneer Max Schrems and his civil society organisation NOYB – European Center for Digital Rights. Nevertheless, the Austrian legal situation has also been considered where possible.

In Germany the rad has been (mainly) transposed in the Consumer Rights Enforcement Act (Verbraucherrechtdurchsetzungsgesetz, hereinafter VDuG).37 According to the German implementation, at least 50 consumers need to be potentially affected by the representative action (consumer quorum, § 4 para. 1 VDuG). The qualified entity can bring a representative action even if it is not yet aware of the number of harmed consumers, instead claiming a (provisional) collective aggregate amount. The procedure is divided into three phases: In the first phase, the qualified entity can obtain a “basic redress decision” (Abhilfegrundurteil, § 16 VDuG), which declares the liability of the trader sued to be justified on the merits. A settlement phase follows, in which

37 “Verbraucherrechtdurchsetzungsgesetz vom 8. Oktober 2023 (BGBl. 2023 I Nr. 272)”. The German Bundestag has passed the VDuG on July 7, 2023 and it entered into force on October 13, 2023.
the parties should strive for an amicable agreement. This requires approval of the court (§ 9 VDuG). If the parties fail to come to a settlement, in the third phase a final redress decision by the court is rendered (§§ 17, 18 VDuG), which is followed by an implementation procedure (§§ 22 ff VDuG).38

In the Netherlands the RAD was implemented through the Dutch Collective Mass Damage Resolution Act (Wet afwikkeling massaschade in collectieve actie, WAMCA),39 which has been in force since 1 January 2020 in Section 3:305a–e of the Dutch Civil Code (Burgerlijk Wetboek) and Section 1018b ff Dutch Code of Civil Procedure (DCCP, Wetboek van Burgerlijke Rechtsvordering). The WAMCA is one of three Dutch collective redress regimes – besides the WCA for injunctive or declaratory relief, and the WCAM collective settlement regime, which became widely known in the Royal Dutch Shell 350 Mio. USD securities class-action lawsuit.40 Compared to the amicable WCAM settlement mechanism, the core innovation of the WAMCA is the court’s power to award damages. The WAMCA-proceeding is initiated by an interest organization bringing a legal action on behalf of its constituency. To be admissible an organization must proof it represents a sufficiently large part of the affected individuals, but there is no stare minimum number of affected persons. The necessary group size is contoured mainly by case law.41 As Dutch collective actions are renowned for their progressive opt-out-mechanisms, this aspect required amendment to comply with the RAD, as it permits opt-outs only for residents of the respective Member State (see supra para. 6.2.). Therefore, consumers domiciled abroad are required to opt-in. In case the opt-out applies, the court sets a first opt-out period. Afterwards the court may order the parties to submit a settlement proposal and stay the proceeding for negotiations (Section 1018i DCCP). If the parties reach a settlement, the judge must approve and declare the settlement binding. In particular, it must be ensured that the amount of compensation is reasonable (Section 1018h DCCP). After such an approval, harmed consumers have a second opt-out opportunity. If no settlement is reached, the proceeding continues to the merit stage (Section 1018g DCCP). There might be a second

38 bt-Dr 20/6520, 61.
41 D. Horemann and M. de Monchy (eds.), Unlocking the WAMCA, 2. Ed. (2022), paras. 124.
4 Data Protection Divergence Across the Atlantic

Strict consumer protection and data protection laws are typical for the EU. Both fields overlap, which becomes apparent in modern, data-driven consumer markets. Yet consumer protection and data protection are rooted in different legal traditions and apply distinct legal concepts. In the EU the main objective of data protection laws are the realization of the fundamental right to data protection, as enshrined in Article 8 of the Charter of Fundamental Rights of the EU (and correspondingly in Article 8 of the European Convention of Human Rights in the context of interpreting the right to privacy in the digital age). In contrast, consumer protection aims to adjust the imbalance between traders and consumers. It is only slightly linked to fundamental rights, rather serving as a social goal during the establishment of the internal market and European integration. Therefore data protection law is distinct
from the European consumer acquis, which has meanwhile grown quite complex.\textsuperscript{48}

In the EU data protection is regulated through the comprehensive GDPR framework. Following the footsteps of the 1995 Data Protection Directive,\textsuperscript{49} the establishment of the GDPR took about 7 years and involved tedious political negotiations next to a multitude of expert consultations to prevent evasion of its regulatory goals.\textsuperscript{50}

Curiously, data protection in the EU and the US share a common root, namely the “Fair Information Practice Principles” (FIPPS), a set of data protection principles articulated in the 1970s in the USA. In Europe the FIPPS were deepened, expanded and applied to all information processing in a principle-based and technology neutral manner (“omnibus approach”).\textsuperscript{51}

In contrast to the EU, in the US data protection is only to a limited extent guaranteed by the constitution (focusing on criminal procedural law). The 4\textsuperscript{th} amendment to the US constitution prohibits unreasonable searches and seizures by the government in private premises.\textsuperscript{52} Yet, the rights granted by the 4\textsuperscript{th} amendment are no equivalent to the EU’s right to data protection, as they only protect citizens in vertical government-vs-individual relations, with its root in the physical domain.\textsuperscript{53} Instead of an omnibus approach as in the EU, the US followed a so-called sectoral approach, where separate privacy related provisions are directed only to specific industries such as healthcare or financial services, leading to a labyrinthine patchwork of state and federal statutes, common law doctrines and industry specific self-regulation guidelines (apart from the recent California Consumer Privacy Act of 2018, see further

The sectoral approach has led to a quite complex legal landscape and recently gave rise to a number of new litigations, where privacy statutes from the telephone, telegraph, and video-cassette eras are leveraged to challenge the use of nowadays routine technologies as unlawful, in order to bring multi-million dollar class-action lawsuits (see further below in para. 6.4.).

In absence of an overarching federal data protection framework and a broad constitutional guarantee of data protection, many forms of information practices remain subject only to general consumer protection law and the Federal Trade Commission's general consumer protection authority. This is a major systemic difference compared to the EU, as US information privacy law explains privacy interest protections with marketplace discourse and conceives it as a type of consumer law. This is well illustrated by many privacy statutes using the term "consumer", such as the prominent California Consumer Privacy Act of 2018 (CCPA), which entered into force in 2020. Despite the diverging concepts, it must be noted that the CCPA has adopted a couple of the legislative ideas of the GDPR (e.g. a right to be informed, right to deletion) and introduces the first (more) comprehensive data protection regime in the US.

From an institutional viewpoint, EU data protection law relies mainly on a public authority-model, with supervisory authorities monitoring and
enforcing the GDPR (Art. 51, 57 GDPR).\textsuperscript{61} In contrast, the sectoral approach implies that there will be no data protection authority with comprehensive competences. Of course, there is the Federal Trade Commission (FTC) who enforces consumer protection laws (and among them data privacy).\textsuperscript{62} However, the FTC is not competent to adjudicate individual data privacy complaints\textsuperscript{63} and its privacy division is said to be understaffed.\textsuperscript{64} This public enforcement gap is filled by private enforcement mechanisms, in particular class actions.\textsuperscript{65} 

The great divide of a strict European and a more lenient US data protection policy sparked a more than 2 decades long controversy about transatlantic data flows.\textsuperscript{66} In the year 2000 the “U.S.-EU Safe Harbor Framework”\textsuperscript{67} was established, allowing the transfer of data from the EU to the US, if US

\begin{itemize}
\item W. Wurmnest and M. Gömann, “Comparing Private Enforcement of EU Competition and Data Protection Law” \textit{Journal of European Tort Law} (2022) 166: “public enforcement by the competent national authorities remains the enforcers’ sharpest blade in the area of European data protection law”.
\item L. Strassemeyer, „Vorhang auf für das Trans-Atlantic Data Privacy Framework – der nächste Akt ist eröffnet“, \textit{DSB} (2023) 186.
\end{itemize}
companies stated to commit themselves to certain privacy principles. Those principles have been invalidated in 2015 in the CJEU-judgement Schrems I,\(^\text{68}\) as the Snowden disclosures questioned the safety of European personal data, especially towards US intelligence authorities.\(^\text{69}\) In 2016 those privacy concerns led to the establishment of a stricter framework, the “EU–US Privacy Shield”.\(^\text{70}\) Yet, also this successor data-sharing deal could not sustain the watchful eye of Maximilian Schrems and the CJEU. The framework has been overturned by the Schrems II judgment of 16 July 2020.\(^\text{71}\) To address this ruling, the “EU-US Data Privacy Framework” (DPF) was negotiated, and the implementation started in 2023.\(^\text{72}\) As its predecessors, it is based on a system of self-certification.\(^\text{73}\) Further, the US adopted an Executive Order,\(^\text{74}\) limiting US intelligence activities to a necessary and proportionate degree.\(^\text{75}\) Whether this latest series of adjusted measures will be sufficient to address the concerns about adequate and effective data protection in transatlantic data flows remains to be seen. Also, the situation may be improved by the recent establishment of the US Data Protection Review Court, investigating and resolving complaints of EU citizens regarding access to their data by US national security authorities.

---

\(^\text{68}\) CJEU judgment of 6 October 2015, C-362/14, Maximillian Schrems v. Data Protection Commissioner.


\(^\text{71}\) Case C-311/18. The CJEU challenged the validity of standard contractual clauses for transatlantic data transfer, again with regard to possible the access by US intelligence authorities; L. Strassemeyer, „Vorhang auf für das Trans-Atlantic Data Privacy Framework – der nächste Akt ist eröffnet“, DSB (2023) 186; M. Schrems, Kämpf um deine Daten (Vienna: edition a 2014); X. Tracol, “Schrems II”: The return of the Privacy Shield, Computer Law & Security Review, Volume 39, 2020, 105-484.


\(^\text{73}\) Commission Implementing Decision of 10.7.2023, para. 9; L. Strassemeyer, „Vorhang auf für das Trans-Atlantic Data Privacy Framework – der nächste Akt ist eröffnet“, DSB (2023) 186.

\(^\text{74}\) Executive Order ‘Enhancing Safeguards for US Signals Intelligence Activities’ (14086) of October 7, 2022.

\(^\text{75}\) L. Strassemeyer, „Vorhang auf für das Trans-Atlantic Data Privacy Framework – der nächste Akt ist eröffnet“, DSB (2023) 187.
Law and Economics of Data Protection Litigation

If damages arise from an infringement relating to personal data, individual claims are typically small, leading to a scattered damage pattern. Data subjects have little interest to enforce such claims individually, as they are confronted with prohibitive litigation costs. Furthermore, empirical evidence (from Austria) shows that only 25 percent of victims have taken out a legal protection insurance and therefore encounter a high risk of substantial legal costs. This leads to so-called rational apathy of affected data subjects. One can imagine that claiming compensation from internet giants such as Facebook/Meta frequently leads to a David v. Goliath-constellation with asymmetrical power relationships. The dilemma is exacerbated by the “privacy paradox”, describing the phenomenon that consumers regard data protection as very important for themselves in principle, but largely ignore data protection aspects in their actual decisions of legal relevance (e.g. “blindly” providing consent to collecting personal data when installing new smartphone apps). As several studies show, data protection declarations are hardly ever read. Due to those market failures traders can achieve considerable injustice-gains.

---

77 RAD Recital 9.
81 For a comprehensive overview of theories and studies on the privacy paradox see S. Barth, M. Jong, “The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review”, Telematics and Informatics 34 (2017) 1038.
Yet, if many harmed consumers can aggregate their claims, the costs per claim decrease and resources are pooled for often lengthy investigations to discover violations, thereby increasing the sophistication of the plaintiffs.\textsuperscript{85} Collective private law enforcement also serves a regulatory and preventive function, as it deters traders from wrongdoing and incentivizes them to obey the law (economic steering effect).\textsuperscript{86}

Another economic problem when enforcing privacy infringements is to measure the value of personal data (valuation dilemma).\textsuperscript{87} Courts are frequently concerned with complex quantification questions relating to the compensation of \textit{non-material} damages.\textsuperscript{88} But also in cases of material damages, such as targeted and personalized ads and price discrimination in online shopping, how can one put a price tag on damages?\textsuperscript{89} In economic terms the provision of personal data has acquired the status of a functional equivalent for monetary payments, which leads to the phenomenon of \textit{data serving as counter-performance} (even though this concept is controversial from a normative perspective). For data subjects decision-making is extremely difficult in such situations, as the appreciation of the real value of their data is

\begin{itemize}
\item \textsuperscript{89} A. Acquisti, C. Taylor and L. Wagman, “The Economics of Privacy”, \textit{Journal of Economic Literature} (2016) 483.
\end{itemize}
distorted by various cognitive biases. This is supported by an empirical study, showing that consumers perceive transactions where they provide their data in exchange for a free service as fair.

Those market failures occurring in data-based consumer markets are aggravated by the leverage effect, as in collective proceedings single damages need to be multiplied by the number of harmed consumers. Slightest mistakes can lead to existential threats for traders.

As final issues to be mentioned, information asymmetries, opacity of data markets and negative externalities often prevent consumers from understanding what is being done with their data. Therefore, as data harms are neither immediate nor visible, data subjects frequently remain unconscious of violations, causing a structural enforcement obstacle.

6 Key Enforcement Questions

6.1 Admissibility of Injunctive and Redress Measures

In representative actions for injunctive measures the practically relevant question arises if a qualified entity is entitled to autonomously file an action, without being mandated by impaired data subjects. Such a scenario is typical for representative actions, as the qualified entity is of separate legal existence from the consumers it represents and statutory authorized to sue.
on its own initiative. The concept of a mandate-free action (in technical terms: *originary competence of intervention*) was already established under the ancient forerunner of the representative action, the Roman *actio popularis*, which granted any citizen the right to bring an action in the public interest.95 In contrast, the class action’s concept – pooling individual claims and an action being brought by the named plaintiff – entails that there is no such originary competence of intervention. For the sake of clarification, US class actions can be initiated by entities such as consumer advocacy groups or data privacy NGOs, which play a key role in data privacy litigation.96 Yet, usually such entities do not possess an originary competence of intervention, and can therefore not sue on their own initiative (without a mandate of their constituency). This would rather apply to public agencies such as the FTC or the California Attorney General under the CCPA97 (see supra para. 4.), which are equipped with certain enforcement powers. This enables them to seek injunctive relief autonomously (respectively *ex officio*) before civil courts. The FTC can also intervene in class actions (as e.g. in the Equifax data breach litigation, see infra para. 6.3).98

Mandate-free representative actions – seeking to cease or prohibit illegal data practices – are valuable from a law and economics-perspective, as they remedy the already mentioned dilemmas of rational apathy, the privacy paradox, as well as frequent unconsciousness of violations (see infra para. 5.). Yet, the question if qualified entities possess such a competence in the context of data protection is of great legal complexity. Chronologically, the predecessor of the Rad – the Injunctions Directive – already provided for mandate-free

---


actions for injunctive relief, but did not address the question if qualified entities can file such injunctive actions without a data subjects' mandate in the context of the GDPR. The German UKlaG (German Act on Injunctive Relief) goes beyond a mere transposition of the Injunctions Directive, and additionally provides for a special data protection injunctive claim (§ 2). It can be initiated irrespective of the infringement of a specific data subjects' rights.

In the preliminary ruling *Meta Platforms Ireland v. Bundesverband der Verbraucherzentralen*, the German Federal Court of Justice (BGH) asked the CJEU if qualified entities could lodge proceedings for breaches of the GDPR independently of the infringement, and without being mandated to do so by a data subject. The BGH was concerned that the GDPR’s wording and the competences of the data protection supervisory authority could preclude the German legislation. One must bear in mind that the GDPR addresses the issue of private enforcement by representative entities (Article 80 para. 1), and confers data subjects the right to mandate certain data protection organisations or associations to exercise rights on their behalf. According to Article 80 para. 2 those representative entities are expressly authorized to file judicial remedies independently of a data subject’s mandate, leading to a certain ambiguity in the interplay with para. 1. Furthermore, it was ambiguous if Article 80 para. 2 also applied to consumer protection associations, notably in a case where it was unclear which of the data subjects' rights had been infringed. The CJEU affirmed that consumer protection associations have standing to

---


104 See also Recital 142 GDPR; M. Federico, “European Collective Redress and Data Protection Challenges and Opportunities”, *Media Laws* (2023) 94 ff.
bring proceedings under Article 80 para. 2 GDPR on their own initiative and that it suffices if the rights of identifiable natural persons have been affected.\textsuperscript{105} The CJEU emphasised how representative actions contribute to strengthening the rights of data subjects and the prevention of infringements.\textsuperscript{106} In addition, the Court made several references to the RAD, suggesting that future representative actions under the Directive will also be compatible with Article 80 GDPR.\textsuperscript{107} It must be noted that the RAD holds a similar provision as the German UKLaG. Here individual consumers seeking injunctive measures are not required to express their wish to be represented by the qualified entity (Art. 8 para. 3 RAD).\textsuperscript{108} However, whether someone is entitled to an injunctive measure (a measure aiming to cease or prohibit a practice) is a question of material law and not procedural law. Therefore, the RAD only serves as a procedural framework to enforce injunctive measures but the entitlement to oblige someone to cease or prohibit a certain practice must be grounded in (national) material law such as the German UKLaG.\textsuperscript{109} To illustrate this with an example, an Austrian consumer association’s lawsuit comparable to the proceeding against Meta Platforms Ireland (cited above) had no standing, as a substantive law-claim for injunctive relief comparable to the one under the German UKLaG lacks in the Austrian Consumer Protection Act (so far, perhaps the gap will be filled in the course of the transposition of the RAD, which is still outstanding).\textsuperscript{110}

\textsuperscript{105} T. Lühmann, P. Schumacher and L. Stegemann, “Gegenwart und Zukunft kollektiver Rechtsdurchsetzung im Datenschutzrecht”, \textit{zd} (2023) pp. 133.


In the Netherlands, according to case law declaratory judgements do not require the mandate of a data subject.\textsuperscript{111} However, a translation ambiguity in the Dutch version of the GDPR (algemene verordening gegevensbescherming, AVG) leaves unclear whether (injunctive or redress) measures require an explicit mandate of the represented data subjects. This question has been raised in the Oracle-Salesforce-ruling of the Amsterdam District Court, which received a lot of media attention but has unfortunately not been adjudicated as the claim was held inadmissible on other grounds.\textsuperscript{112}

Such proceedings show that Member States are – besides the transposition of the RAd – called upon to complement the procedural mechanism by substantive law measures and to fill gaps on the intersection of collective measures and the GDPR. This need for finetuning is also shown by the aforementioned judgment Meta Platforms Ireland v. Bundesverband der Verbraucherzentralen, yet in a different regard. The CJEU reasoned with the improvement of consumer protection, but missed out on possible conflicts between supervisory authorities and qualified entities. This would have been a valid point of concern against the Court’s pro-private enforcement attitude. Many procedural questions on the intersection of data protection and civil procedure are not expressly regulated in EU law and great controversies arise: How should respective regulations and directives be interpreted in this regard? Are parallel proceedings admissible and if so, is there a hierarchy between public and private enforcement?\textsuperscript{113} Will proceedings be suspended in case a court and a supervisory authority deal with the same infringement? Does the quite ambiguous Art. 81 GDPR apply?\textsuperscript{114} How can contradictory decisions be avoided, is there a res judicata effect and which decision is binding on whom?\textsuperscript{115} These dilemmas will be further addressed in para. 6.5. Curiously, in the case Meta Platforms Ireland v. Bundesverband der

\textsuperscript{111} Amsterdam District Court 30 June 2021, Data Privacy Foundation v. Facebook, ecli:nl:rbams:2021:3307, para. 7.32; D. Horemann and M. de Monchy (eds.), Unlocking the WAMCA, 2. Ed. (2022), paras. 339.

\textsuperscript{112} N.M. Brouwer, Lost in translation? De betekenis van artikel 80 lid 2 AVG in verhouding tot de WAMCA Computerrecht 2022/49, 85; D. Horemann and M. de Monchy (eds.), Unlocking the WAMCA, 2. Ed. (2022), paras. 341; Amsterdam District Court 29 December 2021, TPC v. Oracle and Salesforce, ecli:nl:rbams:2021:7647.

\textsuperscript{113} P. Leupold, M. Schrems in R. Knyrim, DatKomm (Vienna: Manz, 2022) Art 79 paras. 31/1.


Verbraucherzentralen another preliminary ruling is pending, in which the CJEU was asked if Art. 80 para. 2 GDPR also applies in constellations where the right to be informed (Art. 13 GDPR) is not complied with.116 Depending on the outcome, this preliminary ruling might broaden the competence of civil courts to rule on the GDPR even further.

6.2 Opt-in v. Opt-out

One of the major crossroads in the RAD-implementation is the decision for an opt-in or opt-out proceeding. In an opt-in mechanism, consumers are required to explicitly express their wish to be represented, whereas in an opt-out mechanism, consumers of a loosely defined group are automatically part of the collective proceeding and bound by its outcome.117

Yet, a distinction must be drawn. For injunctive measures individual consumers are not required to express their wish to be represented (Art. 8 para. 3 RAD), leading to a compulsory participation, which seems justified as injunctive relief is only minimally invasive (see supra para. 6.1).118 In contrast, for “more drastic” redress measures Member States can choose an opt-in or opt-out-mechanism, or a combination of the two (Recital 43, Art. 9 para. 2 RAD). However, opt-out mechanisms are excluded for redress measures where the affected consumers do not habitually reside in the Member State where the representative action is brought (Art. 9 para. 3 RAD).119

National transpositions of the RAD show that most EU-countries prefer the opt-in. Yet, the Netherlands chose the more progressive opt-out-mechanism (see supra para. 3.).120 For several reasons, such an opt-out system could be

---

119 RAD Recital 45.
advantageous to pursue data protection infringements. First, consumers are often unaware of data protection violations. Furthermore, in scatter damage cases, as typically encountered in data protection infringements, harmed consumers show strong rational apathy (see supra para. 5.). The so-called default bias of behavioural economics comes into play, describing the cognitive distortion of people tending to accept default options. Consumer’s reluctance to join a collective proceeding is also empirically proven. Eventually, the opt-out could also facilitate settlements and expedite the proceeding, since the amount in dispute is larger and the chance of consumer claims have lapsed is significantly reduced.

Of course, opt-out-class actions quickly lead to due process-concerns, especially whether consumers have been properly given notice about their inclusion in the class. Nevertheless, this risk should be outweighed in cases of scattered damages by the unpleasant alternative of no enforcement at all. As the RAD sets high standards on the trustfulness of qualified entities, making sure harmed consumers are not deprived of procedural rights, opt-out class actions for scatter damage data infringements would appear justified and proportionate.

Therefore, the Dutch opt-out seems advantageous. Yet, there is doubt if it applies to GDPR-infringements, as Article 37 of the Dutch GDPR-implementation act (Uitvoeringswet Algemene verordening gegevensbescherming) suggests collective redress actions might not be initiated without the consent of represented data subjects. Dutch courts will need to clarify this important question.

---

121 A. Geroldinger, „Rechtsdurchsetzung im Verbraucherrecht – Prozessuale Aspekte“, 21. ÖJF Volume 11/1 (Vienna: Manz 2022) pp. 136. A study of the Austrian Consumer Information Association (Verein für Konsumenteninformation, vki) revealed that consumer damages of at least € 130 are needed to induce 25 percent of the harmed consumers to join a collective proceeding (even though it is free of charge). Study of 2009, inflation-adjusted in the year 2023 approximately € 130.


Regarding the German opt-in – which seems less favourable compared to an opt-out for the reasons stated above – it must be noted that this deficit might be mitigated by a very lenient deadline for consumers to register their claims. They can do so within the first three weeks after the closing of the oral proceeding (§ 46 VDuG).126

6.3 Redress Settlements and Quantification of Damages

Some data protection infringements lead to record compensation. For example, the largest US class-action privacy settlement is purported in the Meta – Cambridge Analytica Lawsuit, where the Facebook parent was accused to allow the now-defunct British consulting firm Cambridge Analytica to access and exploit private information about millions of Facebook-users. According to a court filing end of 2022, Meta has agreed to pay USD 725 million to settle the lawsuit.127 Further, in the Equifax data breach settlement, (at least) USD 575 Million had to be paid for exposing the personal information of 147 million people.128

Experience from the US shows that class actions are regularly not decided by courts on the merits, but the overwhelming majority is settled amicably, according to statistics 90 percent of all US-class actions.129 This settlement tendency is a characteristic of the Anglo-American, adversarial character of adjudication.130 Settlements are particularly likely after admission of the class action at the outset of the trial (class certification), if plaintiffs allege a financial loss and after cyber-attacks.131

In economic terms, settlement negotiations are a private allocation of resources, which can achieve a fair conciliation of interests, provided there is equality of arms among the negotiants.\textsuperscript{132} Such a fair conciliation is uncertain in US class action, as the toxic cocktail of contingency fee agreements and punitive damages (see para. 2.) generates severe settlement pressure.\textsuperscript{133}

The RAD encourages collective settlements. As it aims to avoid the shortcomings of US class action, there might be a fairer conciliation of interests.\textsuperscript{134} The Dutch and the German transpositions tend strongly towards settlements, but they differ in three important aspects: In the Dutch WAMCA the opt-out (for domestic consumers) increases the stake of the claimants in the dispute: As harmed consumers are automatically included in the proceeding, the respondents find themselves confronted with a higher amount in dispute. Therefore, the pressure to settle increases and data protection infringement settlements are facilitated. Further, in the Netherlands the amicable collective settlement procedure (WCAM) permits court approval of pre-arranged settlement agreements, which has no equivalent in Germany. Another difference between the Dutch and the German representative action is the time of the settlement phase. Under the German VDuG, the court renders a “basic redress decision” before the settlement phase,\textsuperscript{135} while under the WAMCA the court suspends the proceeding and invites the parties to settlement negotiations at the outset of the trial, without giving a detailed insight on the prospective outcome of the proceeding.\textsuperscript{136} Experienced trial lawyers might question the ratio of the German basic redress decision, as claimants who can reasonably expect to win a trial are usually better off if they do not settle. Instead, they might let the court decide the case on the merits and compel the


\textsuperscript{135} T. Lühmann, P. Schumacher and L. Stegemann, “Gegenwart und Zukunft kollektiver Rechtsdurchsetzung im Datenschutzrecht”, \textit{ZD} (2023) 132 F. D. Ashkar and C. Schröder, „Aktuelle Entwicklungen im Bereich der Data Privacy Litigation“, \textit{BB} (2023) 454. The basic redress decision entails the amount due to each eligible consumer or, if the amounts due to the eligible consumers are different, the method by which the individual amounts are to be calculated.

\textsuperscript{136} By inviting the parties to settlement negotiations the court of course implies that the claim is not unfounded, see W. van Boom and C. Pavillon, “The Netherlands takes collective redress to a next level”, \textit{VbR} (2019) 135.
defendant to pay the entire claim sum. From this strategic viewpoint, the basic redress decision will not facilitate settlements but rather have the opposite effect. In addition, a drafting error of the German legislator seems to permit collective settlements only at a very late stage of the procedure, after evidence has been taken (§ 17, § 42 VDuG). This would undermine the advantages of settlements, namely to speed up proceedings and to avoid cost and lengthy proceedings.\textsuperscript{137} It will be interesting to see whether the basic redress decision will proof as an efficient tool, but it seems doubtful at this point.

Under the German VDuG judges have wide discretion. If the amount of compensation cannot be determined, the court can estimate it according to its own conviction.\textsuperscript{138} The objective of providing the court with this power is to facilitate the assessment of loss.\textsuperscript{139} Perhaps, the estimation power might induce the litigants to settle, as respondents fear an unfavourable estimation of the damage. As one can imagine, such wide discretion could also be dangerous and open the door to flawed estimations, legal uncertainty, or even misuse of power.

Summarized, in collective actions we encounter various pragmatic procedural mechanisms. Libraries could be filled philosophically analysing if thereby legal certainty and the idea of justice as such might be endangered. Yet, the economic dilemma of very complex damage valuation (see para. 5.) shows the urge of such schematic approaches. Whoever personally witnessed a sophisticated mass damage case would not doubt such a need to reduce complexity.\textsuperscript{140}

6.4 \textit{Non-Material Damages}

A common enforcement obstacle in privacy litigation are non-material damages. Experience from the USA shows that being unable to proof non-material damages is a frequent roadblock for data breach class actions.\textsuperscript{141} In Europe we encounter the same problem, as it is well illustrated by a recent

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{137} G. Vollkommer in: Zöller (ed), \textit{Zivilprozessordnung}, (Köln: Otto Schmidt, 35th issue 2024) § 9 VDuG Rz 5.
\item \textsuperscript{138} § 287 Code of Civil Procedure in connection with § 19 para. 2 VDuG.
\item \textsuperscript{139} bt-Dr 20/6520, 83; D. Ashkar and C. Schröder, „Aktuelle Entwicklungen im Bereich der Data Privacy Litigation“, \textit{BB} (2023) 454; see also, advocating for a broad judicial damage estimation power B. Gsell, C. Meller-Hannich, „Die Umsetzung der Verbandsklagen-Richtlinie als Chance für eine Bewältigung von Streu- und Massenschadensereignissen“, \textit{jz} (2022) 427.
\item \textsuperscript{140} R. Kehrberger, \textit{Die Materialisierung des Zivilprozessrechts: Der Zivilprozess im modernen Rechtssstaat} (Tübingen: Mohr Siebeck, 2019) pp. 7.
\item \textsuperscript{141} J. Black, “Developments in Data Security Breach Liability”, \textit{The Business Lawyer} (2013) 200. Plaintiffs need to show an injury in fact, in order to establish a so-called legal standing under US Constitution Art. III (the constitutional right to bring lawsuits in
\end{itemize}
\end{footnotesize}
decision against the main Austrian provider of postal and logistical services (Österreichische Post AG), which collected information on the political affinities of the Austrian population and generated target group addresses. Subsequently, these profiles were sold to third parties for targeted (election) advertising. In national proceedings before the referral to the CJEU, the claimant demanded compensation for immaterial damages in the amount of EUR 2,500 for having lost control over his data and potentially revealing his political opinions. The Austrian courts dismissed the claim.

In the GDPR the right to receive compensation for non-material damages is expressly stipulated (Art. 82). Currently courts are busy clarifying questions relating non-material damages under the GDPR. As the CJEU ruled in the Österreichische Post-case, on the one hand national laws must not provide for a minimum threshold of damage suffered by the data subject, but on the other hand a mere infringement of the provisions of the GDPR (without damages) is not sufficient to confer a right to compensation.

---

142 Retrieved 31 August 2023: https://perfectlaw.co.uk/ecj-specifies-right-to-compensation-under-art-82-gdpr-in-c-300-21-osterreichische-post/#_ftnref4; CJEU Case C-300/21 – v Österreichische Post AG.
143 OGH 30.06.2021, 6Ob120/21x. The claimant stated to be suffering from ‘an uneasy feeling’ that the defendant has access to information which would not have been voluntarily disclosed.
144 Besides this proceeding, there was (at least) another parallel civil proceeding against Österreichische Post AG, where another claimant demanded EUR 1,000 for falsely being categorized as a rightwing partisan. Also in this cases, the Austrian courts awarded no non-material damage – yet the national final decision after the CJEU’s preliminary ruling is still outstanding, but the chance of succeeding has rather been reduced than improved.
145 Recital 146 GDPR; S. Quaas in H. Wolff and S. Brink, Datenschutzrecht (Munich: C.H. Beck, 2022), Art. 82 para. 33. Also, according to its recitals, the concept of damage should be broadly interpreted in the light of the case-law of the CJEU and in a manner which fully reflects the objectives of the GDPR. Further, data subjects should receive full and effective compensation for the damage they suffered.
The difficulty to determine non-material damages for data protection infringements is a manifestation of the valuation dilemma (see para. 5.). This problem is exacerbated by the procedural difficulty of bundling claims for non-material damages in mass litigation, as a recent interim judgement in the prominent Dutch TikTok-representative action shows: TikTok allegedly infringed privacy rights of children by showing them targeted advertising without their consent. Even though the mass claim is admissible, the Amsterdam District Court stated that the claims for non-material damage could not be bundled as they depend too much on the individual situation of the respective users. This is just in line with theory, as the economic value of data is highly context-dependent and thus varies strongly from person to person.

To our mind, for the reimbursement of non-material damages a pragmatic approach is needed and lump sums could help. They are already well established in the compensation for pain and suffering, in respect of loss of holiday enjoyment, or flight delays and cancellation. In US civil law a similar concept for the reimbursement of damages which are difficult to calculate exists, the so-called “statutory damages”. Several elder privacy statutes (e.g. the Federal Wiretap Act of 1968) provide for such statutory damages. Those dated laws have recently been leveraged in a wave of data privacy class actions to challenge the use of nowadays routine technologies as unlawful, which appears somehow frivolous. Nevertheless, the concept of statutory damages appears...
useful, if used in the context of modern privacy statutes. In this respect the CCPA could serve as a model, which also provides for statutory damages, but there is still room for improvement as it only applies to data breach litigation and not to core data protection rights.\(^{153}\)

Such lump sums could help to ensure that comparable infringements are equally compensated.\(^{154}\) Of course, they could not be set forth by a procedural framework such as the RAD, it would be necessary to enshrine them in substantive law, in particular in legal frameworks such as the GDPR. However, legislation establishing such lump sums would need to be well conceived. A point of reference could be the OECD’s survey of methodologies for measuring the monetary value of personal data.\(^{155}\) In any case, policy makers should avoid creating over-compensation by too generous lump sums (see further para. 6.6).

6.5 Parallel Sanctions Regime of the GDPR

The GDPR is mainly enforced by a sanction regime imposed by national supervisory authorities. Additionally, each data subject shall have the right to an effective judicial remedy for infringements of the Regulation (Art. 79) and compensation for material or non-material damage suffered (Art. 82).\(^{156}\) The RAD supplements this basis for civil damages with a private – collective – enforcement mechanism. Private enforcement is imaginable as a follow-on action, ensuring compensation for damages after official proceedings have been completed, or they can also be an alternative to public enforcement (stand-alone actions).\(^{157}\)

The RAD left the crucial implementation question up to the Member States, if the judiciary or the executive branch (or both) should be competent to hear representative actions (Recital 19 RAD). Making an administrative body competent for collective redress proceedings could simplify many issues arising


\(^{154}\) J. Eichelberger, „Ersatz immaterieller Schäden bei Datenschutzverstoßen“, *WRP* (2021) 166.

\(^{155}\) OECD, Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 223, 18. Indicators based on market valuation (Financial results per data record, Market prices for data, Cost of a data breach, Data prices in illegal markets) and Indicators based on individual (data subjects’) valuation (Surveys and economic experiments, Individual willingness to pay to protect data.)


from the parallel, two-tier- public and private enforcement-system. Yet, public enforcement is often times under the suspicion of lacking impartiality,\(^{158}\) as the national supervisory authorities of Ireland and Luxemburg for example have apparently, in some cases been reluctant to impose fines on their esteemed internet giant-tax payers.\(^{159}\) Also, the concept of a civil proceeding besides an administrative or criminal proceeding is a well-established mechanism known from private enforcement of antitrust-damage or criminal law ancillary proceedings.

In such a dual-track mechanism, the mutual entanglements of public and private enforcement need to be well coordinated,\(^{160}\) but the RAD falls short in this regard (see already para. 6.1).\(^{161}\) In follow-on actions, a myriad of procedural questions will arise, such as a coordination or stay of proceedings, disclosure of evidence on file in proceedings before a national supervisory authority, suspension of statutes of limitations while proceedings before the competition authority are ongoing, or precedent-effect of certain rulings of the national supervisory authority.\(^{162}\) Recently the C\text{JEU} has been concerned with such a dilemma in a case where a shareholder unsuccessfully requested a sound recording of a general meeting and filed both a complaint before the data protection authority and before a civil court (C\text{JEU} C-132/2021, \textit{BE vs. Nemzeti Adatvédelmi és Információszabadság Hatóság}). The C\text{JEU} ruled that those remedies can be exercised concurrently with and independently of each other, and that it was for the Member States “to lay down detailed rules as regards the relationship between those remedies in order to ensure the effective protection of the rights guaranteed by that regulation and the consistent and homogeneous application of its provisions”\(^{163}\)


\(^{163}\) C\text{JEU} C-132/2021, \textit{BE vs. Nemzeti Adatvédelmi és Információszabadság Hatóság}, \textit{ecli:EU:C:2023:2}. 

10.1163/22134514-bja10070 | WÖRLE AND GSTREIN
As the CJEU ruled, and in accordance with the principle of procedural autonomy, it is up to the EU Member States to coordinate the judicial and administrative remedies provided for by the GDPR. Inevitably the discussion about another EU-topic comes to mind, the private enforcement of Antitrust law. The Damages Directive 2014/104/EU was enacted to synchronise antitrust courts with antitrust authorities. It ensured a smooth interplay between private and public enforcement. Unfortunately, the application of the Damages Directive by analogy is not permitted, as there is no indication of an unintended gap between the GDPR and civil procedure. However, for future legislative projects of the EU Member States, interlinking public and private (collective) enforcement of privacy infringements, the respective provisions of the Damages Directive could serve as a model.

6.6 Data Protection Over-Enforcement?

Concluding, a further integration of the GDPR and the RAD – as a procedural mechanism of consumer protection – appears advantageous to solve the GDPR enforcement deficit. Yet, one might speculate if the European concept of the protection of data subjects – here considered from a


consumer perspective – with dissuasive administrative fines and its recent complementation by the strong private law enforcement mechanism, might lead to over-enforcement. Notably, besides its principal purpose of compensating impaired individuals, the RAD also serves a deterring and preventive function (see para. 5.), just like administrative fines. Will this duplication force companies to make disproportionate data compliance expenditures, distracting them from their core business? Will entrepreneurs be deterred from new ventures and experimenting with new business models in fear of GDPR-violations? One must bear in mind that not only social networks – with often limited contribution to public welfare – could be impeded by over-enforcement, but also big data-biotech-companies, for instance. They use highly-sensitive data for the development of new treatments, drugs, and medical applications. However, overshooting effects of administrative fines in combination with the new collective redress mechanism might turn out less threatening in practice, as there are still many and large gaps to fill on the intersection with the GDPR. In particular there are still admissibility questions unsolved (see para. 6.1) and the compensation of non-material damages is many times a roadblock for data protection litigation (para. 6.4). Further, record sum compensation like in the US (see para. 6.3) is not likely to appear in the EU, due to the avoidance of the toxic cocktail (see para. 3.).

7 Conclusion

US class action – an international forerunner in collective litigation – is powerful and controversial at the same time. Its peculiarities result in a so-called toxic cocktail permitting slick attorneys to pursue their own financial interests under the guise of consumer advocates. Therefore, US-style class action – despite its apparent advantages in consolidating claims – should not be “transplanted” to the EU without adaption (see para. 2.).

After an initial hesitance, in the last decades continental European countries also started to enact legal frameworks for collective proceedings. Yet, those national mechanisms are very heterogenous and the EU aims to harmonize them and to implement a minimum standard of collective redress. The RAD seeks to avoid the vices of US class action, in particular by replacing class actions with representative actions, where consumer organizations initiate proceedings instead of profit driven attorneys (see para. 3.).

Data protection under the GDPR encompasses all types of information processing, which is referred to as omnibus approach, whereas the US chose a sectoral approach with separate privacy regimes for specific industries.
(apart from the recent California Consumer Privacy Act of 2018). From a dogmatic perspective, in the EU data protection is based on a fundamental rights-concept, whereas in the US it is perceived from a consumer protection perspective. This corresponds with the institutional viewpoint, where in the EU data protection relies mainly on a public authority-model, while the sectoral approach implies that there will be no data protection authority with comprehensive competences. Hence, private enforcement plays a more vital role in the US (see para. 4). The transatlantic comparison of this article reveals the peril that the EU’s aim to further increase consumer protection by US-inspired private enforcement might collide with the well-established European public authority-model. In the two-tier-system of public and private data protection enforcement a better coordination of proceedings would be required. According to the recent CJEU-judgment C-132/2021, BE vs. Nemzeti Adatvédelmi és Információszabadság Hatóság, and in accordance with the principle of procedural autonomy, it is up to the national laws of the Member States to coordinate the judicial and administrative remedies provided for by the GDPR. The national legislators are therefore called upon to further regulate those difficult procedural matters – the Damages Directive 2014/104/EU, ensuring a smooth interplay of antitrust courts and authorities, could certainly serve as a model (see paras. 6.1 and 6.5).

A characteristic of EU representative actions is that qualified entities are statutory authorized to file for injunctive measures without being mandated by impaired consumers. Therefore, under the RAD individual consumers shall not be required to express their wish to be represented by the qualified entity if an injunctive measure is sought (Art. 8 para. 3). In contrast, the US class action’s concept of pooling individual claims and actions are being brought by the named plaintiff, entails that they are not entitled to sue without a mandate of their constituency. However, for EU representative actions it must be born in mind that the claim for an injunctive measure is a question of material law and not procedural law. Thus, the RAD only serves as a procedural framework to enforce injunctive measures. Therefore, national legislators are called upon to fill the respective gaps, as such an amendment is needed for example in Austria (see para. 6.1).

An opt-out system to pursue privacy infringements would be advantageous for several reasons, in particular as harmed consumers show strong rational apathy in scatter damage-cases and as they are often unaware their rights have been infringed (see para. 6.2).

Experience from the USA shows that the overwhelming majority of class actions are amicably settled. The RAD aims to facilitate settlements, which is well reflected in the German VDuG and the Dutch WAMCA (respectively in the
According to a detailed comparison the Dutch mechanism seems to be more advantageous (see para. 6.3).

A main enforcement impediment for non-material data infringement damages is the valuation dilemma, which is not a procedural problem but an issue for substantive law (and justice theory). This problem is exacerbated by the procedural difficulty of bundling claims for non-material damages in mass litigation, as a recent interim judgement in the prominent Dutch TikTok-representative action shows, where the claims for non-material damage could not be bundled as they depend too much on the individual situation of the respective users. A pragmatic approach such as lump sums – known for example from pain and suffering or loss of holiday enjoyment – could ease the problem. Curiously, in the US a comparable concept (statutory damages) is already provided for in elder privacy statutes, but also the recent CCPA (see para. 6.4).

In conclusion, a further integration of the GDPR and the RAD – as a procedural mechanism of consumer protection – appears advantageous to solve the GDPR enforcement deficit. Yet, one might speculate if the GDPR’s dissuasive fines and their recent complementation by the strong private law enforcement mechanism of the RAD might lead to over-enforcement. Of course there is reason for such concern, but the overshoot might be kept within limits due to certain imperfections on the intersection of data protection law and collective litigation. In particular, there are still admissibility questions unsolved, and the compensation of non-material damages remains a major roadblock for data protection litigation. Finally, record sum compensation like in the US is not likely to appear in the EU, due to the avoidance of the toxic cocktail (see para. 2.).