Max Planck Institute
LUXEMBOURG
for Procedural Law

Max Planck Institute Luxembourg for Procedural Law
Research Paper Series | N° 2019 (3)

Procedural Harmonization and Private Enforcement in the Area of Personal Data Protection

Prof. Dr. Marta Requejo Isidro
Senior Research Fellow
Max Planck Institute Luxembourg
for Procedural Law

www.mpi.lu

The 'MPI Luxembourg for Procedural Law Research Paper Series' gathers pre-publication versions of academic articles, book chapters, or reviews as well as intermediary research reports on various legal issues. All manuscripts are offered on the Institute's website as well as our SSRN webpage and are released by each author in the interest of advancing scholarship.

The quality of the research papers is guaranteed by a rigorous internal review, and final approval is given by at least one of the Directors of the Institute. The content is the responsibility of individual authors. Papers may be downloaded by individuals, for their own use, subject to the ordinary copyright rules.

Max Planck Institute Luxembourg for Procedural Law Research Paper Series
ISSN: 2309-0227

Max Planck Institute
LUXEMBOURG
for Procedural Law

4, rue Alphonse Weicker
L-2721 Luxembourg
www.mpi.lu

PROCEDURAL HARMONIZATION AND PRIVATE ENFORCEMENT IN THE AREA OF PERSONAL DATA PROTECTION

Marta Requejo Isidro

Max Planck Institute Luxembourg for Procedural Law, marta.requejo@mpi.lu

Article last updated: February 2019

Abstract: Individuals' control over personal data has a role to play in the field of data protection. The GDPR offers to the data subject a number of possibilities to manage his/her data and to keep the control on them; in this way it helps building up a feeling of empowerment. By recognising the rights of access, rectification, erasure, and data portability of the data subject, and imposing on controllers and processors limits to the processing as well as obligations of information, the European GDPR endorses the protagonism of the individual. At the level of enforcement, however, the EU legislator unambiguously privileges the public mechanisms. Whereas in the GDPR private enforcement is addressed and improved relative to the situation under Directive 95/46/EC, it stays relegated to a discrete second place; as a consequence, the harmonization of the corresponding procedural rules remains restricted as well.

Keywords: personal data protection; private enforcement; harmonization of procedural rules

Cite as

Marta Requejo Isidro, 'Procedural Harmonization and Private Enforcement in the Area of Personal Data Protection' (2019) MPILux Research Paper Series 2019 (3) [www.mpi.lu].

An updated version of this paper will be published in a collective book compiling the presentations at the MPI-UCM joint seminar *Harmonization of Civil Procedure in the EU: How Far Can We Go?*, July 19th, 2018.

1 Introduction

Article 8 of the Charter of Fundamental Rights of the European Union, in Chapter II ('Freedoms'), recognises the right to data protection as an independent right. The right exists as well in the Treaties, under Article 16.1 TFUE. [1] In the secondary legislation, already in the 90's some pieces had been enacted in relation to natural persons' data, with the double objective of harmonizing the protection of the right in respect of processing activities and ensuring the free flow of data between the Member States. The most relevant pieces of legislation in this regard were Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;[2] and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997, on the processing of personal data and the protection of privacy in the telecommunications sector.[3] The latter was repealed in 2002 by Directive 2002/58/EC, on privacy and electronic communications (the 'cookies' Directive),[4] amended in turn in 2009 by Directive 2009/136/EC.[5] A Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), is pending.[6] Directive 95/46/EC has been repealed by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, GDPR, which entered into force in 2016 and is fully applicable since May 25, 2018.[7] It is worth noting that pursuant to the Explanatory Memorandum to the Proposal for a Regulation on Privacy and Electronic Communications "All matters concerning the processing of personal data not specifically addressed by the proposal are covered by the GDPR"; in addition, some provisions of interest for the purposes of this paper refer directly to the GDPR.[8]

While the GDPR acknowledges that the principles underlying Directive 95/46/CE remain sound, the need was felt to enact new rules for two reasons. First, the rapid technological developments and globalisation had brought new challenges for the protection of personal data. Secondly, the Directive had not succeeded in preventing fragmentation in the implementation of data protection across the

---

[1] Former Article 286 TEC: the contents of the new provision are nevertheless notably different.

[2] OJ L 281, 23.11.1995.

[3] OJ L 24, 30.1.1998.

[4] OJ L 201, 31.7.2002.

[5] OJ L 337, 18.12.2009.

[6] COM/2017/010 final - 2017/03.

[7] OJ L 119 4.5.2016. Further instruments address the protection of personal data in specific domains: see the Directive (EU) 2016/680 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016). Not personal data. Regarding non-personal date see the recent Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018.

[8] See Article 21 (referring back to Article 77, 78 and 79 GDPR), Article 22 (to Article 82; the actual scope of the reference may be discussed). There is no provision on representative actions (Article 80 GDPR); Article 21.2 may be understood as equivalent - to a limited extent.

Union.[9] As a reaction the GDPR sets out in detail and reinforces the rights of data subjects, it emphasises the obligations of controllers and processors, and provides for powers to ensure compliance with the rules, and sanctions for infringements, equivalent in all Member States.

The 'provision for powers' just mentioned is not only addressed to the public authorities; it benefits the data subject too. Scholars claim the GDPR strengthens the right to an effective judicial remedy and facilitates private enforcement actions.[10] At a first glance, in view of provisions such as Article 79 (right to an effective judicial remedy) or Article 80 (representative actions), the opinion can be shared. Furthermore, it could be added that by offering to the individual procedural tools to support the defence of his/her right in court, the GDPR contributes to the harmonization of civil procedural law within the EU. At a second look, however, it appears that the impact of the GDPR may not be so significant, neither in relation to private enforcement nor to procedural harmonization. In what follows we will present the pertinent GDPR rules in context; at a second stage we will assess them from the perspective of their relevance both to private enforcement and to the harmonization of procedural rules in the EU.

2 Status quo prior to May 25th, 2018

Already under Article 22 Directive 95/46/CE (Remedies), Member States were obliged to make a judicial remedy available for any breach of the rights guaranteed by the national law applicable to the data processing. Article 23 of the Directive (Liability) addressed the right to compensation from the controller in case of damage having been suffered as a result of an unlawful processing operation, or of any act incompatible with the national provisions adopted pursuant to the Directive. But, in spite of these possibilities, private enforcement was very seldom used to support data protection: scholars' writings,[11] as well a survey conducted on 16 Member States on the access to data protection remedies in EU Member States by the EU Agency for Fundamental Rights, FRA,[12] show that very few victims of data protection violations filed for an injunction or for compensation - to the point that some of the interviewees could not even recall one single civil case on the subject matter during their careers.[13] At the theoretical level this may be explained by a conceptual hesitation in the Directive: entitled '(Directive) on the protection of individuals with regard to the processing of personal data and on the free movement of such data', its recitals refer to the protection of 'fundamental rights and freedoms', adding 'notably the right to privacy' (Recital 2, 7, 10, 11, 68; see as well Article 1). However, data protection and privacy are different rights; a violation of the former may perfectly take place without touching upon the latter.[14] Personal data protection can actually be described as a 'hybrid'. On the

[9] The EU focus regarding personal data has always combined the concern to facilitate the free flow and trade of data (in light of its direct impact in other economy sectors, such as the purchase of services and goods on line) with the fundamental right approach.

[10] Recently L. Lundstedt, 'International Jurisdiction over Cross-Border Private enforcement Actions under the GDPR', Stockholm Faculty of Law, Research Paper Series no 57, at 214.

[11] See D. Korff, 'New Challenges to Data Protection Study - Comparative Chart: Divergences between Data Protection Laws in the EU' (February 15, 2010). European Commission DG Justice, Freedom and Security Report. Available at SSRN: https://ssrn.com/abstract=1638951 or http://dx.doi.org/10.2139/ssrn.1638951 (last visited 14.02.2019). L. Bygrave, *Data Privacy Law*, OUP, 2014, at 178.

[12] https://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states (last visited 17.02.2019).

[13] FRA Study (fn. 12), at 32, referring to Finland. L. Bygrave (fn. 11): national courts are increasingly generating data privacy jurisprudence, but the development is slow.

[14] See O. Lynskey, *The Foundations of EU Data Protection Law*, OUP, 2015, in particular Part I, Chapter 4, on the relationship between data protection and privacy.

one hand, it works as a guarantee for other fundamental rights, particularly the right to privacy; in combination, the protection of privacy and of personal data underpin the right to a private life and the individual's dignity. On the other hand, the right to personal data protection is an independent right: in the face of the threats derived from the new technologies personal data protection is needed to further the scope of protection provided by traditional rights, but also to ensure personal freedom. Here, the fundamental right to personal data protection goes beyond the boundaries of privacy and is not any longer instrumental to it;[15] it involves the empowerment of the individual to control the access to, and the availability of, personal information, and can thus be referred to as 'right to informational self-determination'. This dual dimension[16] of the protection of personal data was not clear under Directive 95/46/CE. The ambiguity is likely to account for the difficulties in identifying the violations and associated harms in the domain of data protection as legally actionable *per se*.

In practice, in their path to the civil courts data subjects faced multiple obstacles, both legal and factual. Personal data protection breaches are often 'hidden': the data subject only becomes aware as a result of further problems experienced in his daily lives.[17] In a similar vein, data protection violations do not necessarily result in a financial loss: the common harms of data processing are intangible - 'a feeling of helplessness and unease', due to the information asymmetries between the controllers and processors and the individuals whose data are processed; a 'chilling effect on individual behaviour', consequently to the impression of being monitored and under surveillance; the 'erosion of the ability of the individual to self-present' in a manner they are comfortable with; the apprehension of future harm-.[18] The very type of damage may work as a barrier to claim redress: individuals may not identify the harm as actionable; they may prefer to forget the situation for fear of worsening it, and/or have concerns about anonymity and confidentiality. Often, the perception that the controller or processor is too powerful, and the offence too frequent to be socially considered as real violations, deter the data subjects from going to court.[19] Particularly in some member States the amount of damages awarded for data protection violations actually supported this conviction of unworthiness: for instance, before 2014 the greatest award for distress in an English reported case was £750 with a nominal £1 for financial loss.[20]

In addition to the factual obstacles procedural hindrances played a role as well in the decision not to sue or to claim for compensation: common factors accounting for self-restraint were the duration of the civil proceedings; the costs - to be borne, at least initially, by the claimant; unforeseeable, but presumably high, especially due to the need to hire a lawyer familiar with a complex subject matter -; or the difficulties related to the gathering of evidence and to the burden of proof -in particular regarding internet-based activities.[21] It is interesting to note that in some legal systems a private law

---

[15] In this sense already in the 90's, the decision of the Spanish Constitutional Court 254/1993, 20.07.1993, *BOE* No 197, 18.08.1993, para 6 of the legal grounds.

[16] For a third theoretical approach to data and data protection, in support of regulating data as property see J. Ritter, A. Mayer, 'Regulating Data as Property: A New Construct for Moving Forward', 16 Duke L. & Tech. Rev. 220.

[17] *Id. loc.*, p. 27. O. Lynskey (fn. 14), at 212.

[18] O. Lynskey (fn. 14), Chapter 6, under E. See as well FRA Study (fn 12), under 3.2. Reported financial damages are usually of minor importance; they relate to refusal of access to credit, financial losses due to identity theft, and costs incurred on telephone calls, postage and having records accessed and amended.

[19] FRA Study (fn. 12), at 30-31.

[20] See S. Atkinson, 'Privacy and data protection cases: quantifying damages for distress', 23.02.2017, https://www.brownejacobson.com/training-and-resources/resources/legal-updates/2017/02/privacy-and-data-protection-cases-quantifying-damages-for-distress (last visited 13.02.2019).

[21] FRA Study (fn. 12), under 4.1.

action for data protection infringements is not of long date - or does not even exist-; the same goes for the type of actionable damage.[22]

3 The GDPR : from 25 May 2018 on

3.1 'Putting individuals in control of their personal data'

In its Communication entitled 'Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century', of 2012,[23] the Commission acknowledged that individuals '(…) feel they are not in control of their data. They are not properly informed of what happens to their personal information, to whom it is transmitted and for what purposes. Often, they do not know how to exercise their rights online.' As consequence, new legislative acts were needed 'to strengthen rights, to give people efficient and operational means to make sure they are fully informed about what happens to their personal data and to enable them to exercise their rights more effectively.'[24]

The GDPR takes up and gives legislative shape to the individual's control over personal data principle. At the substantive level, it strengthens existing subjective rights and provides for more in Chapter III: the right of access, the rights to rectification and erasure, the right to obtain from the controller restriction of processing, the right to data portability, to object to the processing of personal data, and not to be subject to a decision based solely on automated processing, including profiling; both the right to obtain restriction of processing -Article 18- and to data portability -Article 20- are new. The obligations of controller and processor, grouped largely under Chapter IV, are increased and refined. Of the outmost relevance are the rules on information -what it encompasses; how it shall be communicated-, enabling the data subject to exercise his/her rights. Regarding the minimum information that data controllers must convey about the collection and processing of data received from the data subject, or from third parties, by explicit mandate of Article 12 the controller shall take appropriate measures to provide it in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular when the information is addressed specifically to a child. The right of access of the data subject under Article 15 is fine-tuned relative to Directive 95/46/CE: data subjects are entitled to information such as the envisaged period for which the personal data will be stored (or the criteria used to determine that period), or the source of the data when they have not been collected from the data subject. In addition, according to the same provision the controller shall provide for free a copy of the personal data undergoing processing for free. Article 17 sets out the circumstances for the exercise of the right to erasure, and as a complement Article 19 imposes on the controller the obligation to communicate any rectification or erasure of personal data, or restriction of processing, to each recipient to whom the personal data have been disclosed.

Further provisions secure the position of the data subject *vis-à-vis* the controller, but also the processor. For our purposes one of the most relevant rules in this regard relates to the right of compensation and liability: according to Article 82 (Right to compensation and liability), any person who has suffered material or non-material damage as a result of an infringement of the Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

---

[22] D. Svantesson, 'Enforcing Privacy Across Different Jurisdictions', in: D. Wright, P. de Hert (eds.), *Enforcing Privacy. Regulatory, Legal and Technological Approaches*, Springer, 2016, 195-222, at 211, 214.

[23] COM(2012) 9 final, 21.01.2012.

[24] *Loc. ult. cit.*, at 6.

In order to ensure obedience to the rules the GDPR provides as well for enforcement mechanisms under Chapter VIII, including a private prong. Pursuant to Article 79 the data subject has a right to an effective judicial remedy against a controller or processor; the right to compensation for damages, as well as rules on liability, is set up on Article 82 as indicated.[25] Both provisions find an immediate precedent in the Directive 95/46/EC: the former corresponds to Article 22, the latter to Article 23. The scope of the current rules, in particular of Article 82, is nevertheless much broader. Moreover, the Regulation backs private claims with procedural tools which were not foreseen under the Directive. Conceptually, enhanced private enforcement represents another step towards the empowerment of individuals, in line with the very essence of the fundamental right to personal data protection.

3.2 Procedural tools

Along the GDPR several rules pertaining to (civil) procedure can be identified, and grouped as follows.

3.2.1 Regarding cross-border litigation and parallel proceedings

Directive 95/46/CE did not include any rule on international jurisdiction.[26] As a consequence, the grounds for jurisdiction were to be found in other EU Regulations - in particular, in Regulation (EU) No 1215/2012, of the European Parliament and of the Council,[27] or the instruments preceding it, as interpreted by the CJEU- when applicable; otherwise, in the legal systems of the Member States. On the contrary, pursuant to Article 79.2 GDPR, 'Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence (...).' Recital 145 makes it clear that the choice is given to the plaintiff. Recital 147 explains that general jurisdiction rules such as those of Regulation (EU) No 1215/2012 should not prejudice the application of the GDPR specific rules.

Additionally, the GDPR anticipates in Article 81 a situation of parallel proceedings pending before competent courts in different Member States. Courts are instructed to get in contact to confirm that the existence of concurring proceedings; should this be the case, any court other than the one first seized may suspend the proceedings; if the proceedings are pending in the first instance, the court may decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof. The wording of the provision is all inclusive: at least at first sight it could be equally applied to judicial proceedings for a remedy against a decision of a supervisory authority, or for a civil remedy between private parties.

[25] Private enforcement refers typically to litigation in the courts; however, other alternative mechanisms are available and may get to the desired outcome in a quicker and less expensive manner. The GDPR is quite succinct in this respect: out-of-court procedures are just mentioned as a possible content of codes of conduct to be prepared by associations and other bodies representing categories of controllers or processors for the purpose of specifying the application of the Regulation; they shall no prejudice the rights of data subjects pursuant to Articles 77 and 79 (Article 40.2.K GDPR). The Regulation is vague as well about the implementation procedures of the right to rectification (Article 16) or the right to erasure (Article 17), which are acknowledged but not coupled with a common procedure for having them enforced; as a consequence controllers choose their own ways to comply.

[26] In terms of applicable law, Article 4 addressed the delimitation -territorial scope- of the EU national provisions adopted pursuant to the Directive. It could therefore be understood as a conflict of law rule (incomplete, though: for instance, the case of a controller established in several Member States was not solved).

[27] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 351, 20.12.2012.

3.2.2 Regarding legal standing

Pursuant to Article 80 GDPR,[28] not-for-profit body, organisation or associations satisfying specific requirements are entitled to exercise the right to lodge a complaint with a supervisory authority, and the right to a judicial remedy (against a supervisory authority, or against a controller or processor) of the data subject on his/her behalf. Where provided for by Member State law and subject to the mandate from the holder of the right, the above listed bodies may also exercise the right to receive compensation.

3.2.3 Regarding evidence

Several provisions of the GDPR can be read as relating to evidence and proof.

Article 5 GDPR, on the principles relating to processing of personal data, lays down the principle of 'proactive responsibility', which encompasses both actual compliance with data protection principles and obligations, and - more relevant for the purposes of this paper- the ability to proof it: 'The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1'. Further provisions in the operative text of the Regulation tune up the obligations of controller and processor stressing anew the need to be able to demonstrate compliance. Moreover, the Regulation lists features which may be used as elements in the demonstration. In particular, adherence to approved codes of conduct (in the sense of Article 40, 'Codes of conduct') or approved certification mechanisms (in the sense of Article 42, 'Certification') may be used as an element by which to demonstrate compliance with the obligations: see Article 24.3, Article 25.3, Article 28.5, Article 32.3, Article 35.8. The same idea appears in the Recitals: when the processing is to be carried out by the processor on behalf of the controller, the adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller and/or processor (Recital 81).

Pursuant to Article 6 the lawfulness of data processing is conditional upon several requirements, one of them being the consent of the data subject. Should processing be based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data (Article 7, Recital 42). Moreover, consent must be freely given; it will be presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance (Article 7, Recital 43).

As a rule, a controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22 even in cases where processing does not require identification of the data subject for the purposes of complying with the Regulation; however, the controller will be exempted it he demonstrates that it is not in a position to identify the data subject (Article 12.2). Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may charge a fee or refuse to act on the request; it shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request (Article 12.5.)

[28] See as well Recital 142.

Article 21 GDPR establishes the right to object of the data subject. In case of objection the controller shall no longer process the personal data unless he demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.[29]

According to Article 82, on the right to compensation and liability, a controller or processor shall be exempt from liability for the damage caused by processing which infringes the Regulation (the controller), or where it has not complied with obligations of the Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller (the processor), if it proves that it is not in any way responsible for the event giving rise to the damage.

3.2.4 Regarding remedies

Data subjects have the right to file a claim before the competent courts of the Member States in accordance with Article 79, and to obtain redress and compensation following Article 82. Pursuant to the latter, the claim for compensation may be lodged by any person who has suffered material or non-material damage as a result of an infringement of the Regulation, against the controller and/or the processor. As stated above, it is not impossible to be exempted from liability but the standard of proof is high: a controller or processor must prove that it is not *in any way* responsible for the event giving rise to the damage (italics added).

On the scope of the remedy, according to Recital 146 the concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice, in a manner which fully reflects the objectives of this Regulation.

4 Assessment

4.1 In terms of procedural harmonization

To some extent the GDPR is a Regulation worded as a Directive. It expressly grants a margin of manoeuvre for Member States to specify -even to restrict- its rules in relation to particular areas of data processing (see for instance Recital 10, Recital 129).[30] Divergence at the level of the implementation of the Regulation is to be expected as a consequence of open-ended or incomplete provisions which - for the purposes of the judicial application of the rules- are an invitation to the procedural autonomy of the Member States. Uniform interpretation may prove to be difficult too.

4.1.1 Rules on international jurisdiction and parallel proceedings

Article 79.2 GDPR is a clear provision only on the surface. Its wording actually casts doubts on how it relates to other grounds of international jurisdiction (particularly those of the Regulation (EU) No 1215/2012), and the extent to which the latter remain available. Indeed, there are situations not covered by Article 79 GDPR, thus where the 'general rules' could still apply. An example would be a dispute involving a data subject without residence in the EU but who *is* in the EU, and a controller

[29] See as well Recital 69: '(…) It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.'

[30] That is why Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of the Regulation into their national law (Recital 8).

without an establishment in any EU member state; the processing of the data of the former may still fall under the scope of the GDPR pursuant to Article 3.2,[31] but none of the grounds of Article 79.2 are given. Interpretative doubts arise as well about the meaning of 'establishment' -scholars claim that the Regulation, by using in Recital 22 the same wording as Directive 45/96/CE, takes up the case law of the CJEU on the latter[32]-, and of 'habitual residence' of the data subject,[33] which may end up in opportunities for the 'general rules' (such as the place where the place where the harmful event occurred or may occur, Article 7.2 Brussels I bis Regulation) to apply.

Moreover, in light of the ECJ case law on the interpretation of the grounds for jurisdiction set up for the protection of weak parties in cross border litigation, whether a representative action in the sense of Article 80 GDPR can be brought before the court of the habitual residence of one or several of the represented data subjects is disputable.[34]

Moving to the rule on parallel pending proceedings, Article 81, in light of the wording the provision could apply both to judicial proceedings for a remedy against a decision of a supervisory authority, or for a civil remedy between private parties. Recital 144 points to a different understanding, though: literally it restraints the scope of the rule to a situation 'where a court seized of proceedings against a decision by a supervisory authority has reason to believe that proceedings concerning the same processing, such as the same subject matter as regards processing by the same controller or processor, or the same cause of action, are brought before a competent court in another Member State.'

4.1.2 Rules on standing (and on the identification of the defendant)

On the side of the claimant, Article 80 on representative actions is a GDPR example of an open provision implemented (or to be implemented) in the Member States in different ways. A comparative analysis of several EU systems concludes that, as expected,[35] the conditions regarding standing to sue of the interested not-for-profit bodies, organisations or associations differ. In addition, as of today some member States offer broader rules on standing than the GDPR - eg, the Spanish model allows representative entities to bring actions for compensation without having been mandated by the data subject; standing to sue benefits a number of actors not referred to by Regulation, such as groups of individuals gathered *ad hoc*, just for the purposes of bringing a claim;[36] in the UK a representative

[31] 'This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.'

[32] M. Gömman, 'The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement', 2017 (54) Common Market Law Review 567, 570-574; P. de Miguel Asensio, 'Aspectos internacionales de la protección de datos: las sentencias Shrems y Weltimmo del Tribunal de Justicia', (2015) 31 La Ley Unión Europea; *id.,* 'Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea', (2017) 69 Revista española de Derecho internacional 75, para. 12

[33] At the EU level there is no single definition of 'habitual residence', but one which may vary depending on the legal context (family law, child abduction, social security law...) where it is used.

[34] See Case C- 498/16, EU:C:2018:37; M. Requejo Isidro, 'Max Schrems Against Facebook. CJEU, case C-498/16', MPI Working Paper series, 2018 (4), at 10.

[35] See already M. Requejo Isidro ' La aplicación privada del derecho para la protección de las personas físicas en materia de tratamiento de datos personales en el reglamento (UE) 2016/679' (2017) 42 La Ley Mercantil, under III.2.a.

[36] M. Requejo Isidro, *loc. ult. cit*; A. Pato, 'The Collective Private Enforcement of Data Protection Rights in the EU', pending publication in Cadiet/Hess/Requejo (eds), *Privatizing Dispute Resolution and Its Limits,* Nomos, under 2.2.

claim may be filed by an individual on behalf of a class (although after *Lloyd v Google LLC* the conditions of availability will certainly not be easy to meet.)[37]

Still on the claimant, it should be noted the difference in the wording between Article 79 on the right to an effective remedy, which benefits the data subject, and Article 82 on the right to compensation, where the entitlement is general ('Any person'). The lack of any explanation may result in a divergent application of the provisions in the Member States.

On the side of the defendant, difficulties and discrepancies are predictable having in mind the vagueness of the category -in particular that of 'controller'-, still in the process of determination. Indeed, a definition has been arranged for in the Regulation, Article 4.7 (for the controller) and Article 8 (for the processor). However, as we will see below, the real problem does not lay with the lack of a legal concept, but rather on the identification of those falling under its scope for the purposes of the allocation of responsibility.

4.1.3 Rules on evidence

The exact implications of the requirement that controllers must 'be able to demonstrate compliance', which appears all along the GDPR, are unclear. To start with, the Regulation does not state whether the obligation exists *vis-à-vis* the data subject or (and?) the supervisory authorities.[38] As a consequence, to the question whether the duty is tantamount to a reversed burden of proof, scholars give different answers : 'On peut se demander si cette répartition de la charge de la preuve n'est pas modifié du fait de l'existence d'un nouveau principe introduit par le RGPD.'[39] Conclusions differ from the assertion 'Since pursuant to para.1 [Article 7] the controller bears the burden of proof for the issuance of consent and its scope (…)',[40] to '[the obligation to demonstrate compliance] does not result in a shifting of the burden of proof (…) [Since] accountability is not a right of the data subject (…) , the ability to demonstrate compliance is not a legal obligation but may help to fulfil the burden of proof';[41] 'At the very least, the argument can be made that the provisions of the GDPR regarding accountability (…) reinforce the notion that the controller is in fact 'best placed' to proffer evidence of the measures it has taken to ensure compliance. Even if the legal burden of proof is still borne by the data subject, the

[37] [2018] EWHC 2599 (QB). In the case at hand Google was sued for its role in the collection, collation, and use of data obtained via the Safari Workaround, and for breach of duty. The claim was brought in reliance on CPR 19.6, which is headed 'Representative Parties with the Same Interest'. The Court analysed on its own motion whether the parties had the same interest and concluded they had not. In addition, it appreciated insuperable practical difficulties in ascertaining whether any given individual is a member of the Class; further and alternatively, the Court's discretion would in any event be exercised against the continuation of the action as a representative action. Compare with the US: for an on-going class action complaint in the US for security breach, *Echavarria et al. v Facebook Inc*, Case 3:18-cv-05982, available at: https://www.pacermonitor.com/public/case/25776427/ECHAVARRIA_et_al_v_Facebook,_Inc (last visited 16.02.2909)

[38] *A priori*, its violation could be sanctioned with a fine pursuant to Article 83 (see nonetheless A. Ingold, « Article 7», in : Sydow (ed.), *Europaïsche Datenschutzgrundverordnung,* 2nd ed., Nomos, 2018, 445, para. 53, claiming it may be a disproportionate reaction). Additionally, Article 30.4 and Recital 82 could be read as limiting the duty to the relationship of the controller with the supervisory authorities.

[39] K. Rosier, A. Delforge, 'Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD », in: Terwangne/Rosier (dirs.), *Le Règlement Général sur la protection des Données (RGPD)*, Larcier, 2018, 665, 682.

[40] L. Feiler, N. Forgó, M. Weigl, *The EU General Data Protection Regulation* (GDPR): *A Commentary,* GLP, 2018, p. 87 (bold in original). In the same lines, A. Bensoussan, *Tèglement Européen sur la Protection des données*, 2nd ed., Bruylant, 2018, 105.

[41] L. Feiler, N. Forgó, M. Weigl (fn. 40), at 76.

evidential burden of proof should de facto shift to the controller as soon as the data subject has offered prima facie evidence of an unlawful processing activity'.[42]

4.1.4 Rules on remedies

The GDPR is silent regarding relevant aspects of civil remedies; different interpretations and/or implementations are thus to be expected. For instance, no reference is made to preventive measures: literally they are not admissible under the GDPR,[43] for according to Article 79 data subjects shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation *have been infringed* as a result of a processing in non-compliance with the Regulation (italics added).

Regarding injunctions, doubts are likely to arise regarding the territorial scope of the obligation to erase or to rectify personal data. They have been left to be decided by the courts, or by the CJEU.[44]

Moving to compensation - Article 82-, there is no mention in the GDPR to treble or punitive damages awards, neither to include nor to forbid them. Recital 146 could be read as pointing to the exclusion - 'Data subjects should receive full and effective compensation for the damage they have suffered'-, but a different understanding could be supported by another sentence of the text- 'The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation'. Indeed, the assertion might only relate to the concept of damages encompassing material and non-material ones (as expressly stated under Article 82), in order to avoid doubts about the latter: it is worth recalling that awards of moral damages in the field are not of long date in some Member States.[45]

Still on compensation, the wording of Article 82 is unclear as to whether the mere violation of data protection rules, without any additional harm, could be a ground for a claim for compensation.[46] Furthermore, the provision does not address the calculation of damages in spite of the very different practices in the Member States (in some the calculation methods are established by the lawmaker; in other they are left to the courts), especially in relation to moral damages.[47]

---

[42] Van Alsenoy, B., 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation', (2016) JIPITEC 271, under 3.1.3.

[43] Preventive measures are addressed in Recital 137, Article 62.7, Article 66, in the context of joint operations of supervisory authorities and the consistency mechanism.

[44] See the conclusions of AG Szpunar to case C-505/17, EU:C:2019:15, 10.01.2019. See as well case C-18/18 (hearing 12.02.2019).

[45] The typical example is the UK, see *Google Inc. V. Vidal Hall*, [2016] QB 1003, [2015] EWCA Civ 311.

[46] In favour, Center on Regulation in Europe (CERRE), Consumer privacy in network industries - a CERRE policy report, 25.01.2016, available at: http://www.cerre.eu/sites/cerre/files/160125_CERRE_Privacy_Final.pdf, p. 58. The recent UK decision *Lloyd v. Google* [2018] EWHC 2599 (QB), para 55 ff. - still applying the Data Protection Act 1998- would point to the contrary.

[47] A. Galetta, P. de Hert, 'The Proceduralisation of Data protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-oriented Remedial System', 2015 Review of European Administrative Law 125, 149, regret that the EU lawmaker has neither fixed thresholds for compensation awards, nor established any other tailored way of compensation, for instance in the lines of those existing for passengers' rights.

4.2 In terms of private enforcement

4.2.1 Preliminary evaluation

Private enforcement rests on the will and initiative of the individuals to go to court. Generally speaking, procedural tools supporting such will and promoting private enforcement can be grouped in three categories:

a. Regarding access: representative actions; rules on costs and on fees; funding opportunities; disclosure.

b. Regarding incentives to engage in litigation (for parties and lawyers): rules on remedies (damages, particularly opening the door to punitive or treble damages; privacy-specific remedies, such as those to restore a reputational harm).

c. Regarding empowerment for litigation: they relate to evidence, means of proof, burden of proof, standard of proof, discovery; also, to the interaction between private/public enforcement (follow-on actions, evidentiary value of administrative decisions in civil procedures).

Having in mind those elements, and particularly if compared to the legal frame under Directive 95/46/CE, the GDPR may be regarded as a step forward. The rules on disclosure and information, representative actions, international jurisdiction, or evidence, place the data subject in a much better position to defend his/her rights than before. Suffice it to recall a case like *Richardson v Facebook*, where the claimant applied for permission to appeal against a master's rejection of her claims for damages for libel and breach of her right to respect for her private life, and for a question to be referred to the European Court of Justice for a preliminary ruling.[48] She had brought actions after a profile and a blog, which purported to have been created by her but which she maintained were fakes, were published on two website; under this profile personal information had been posted relating to the claimant, and various allegations were made concerning her private life. The master rejected her claim regarding the profile on the first website because the corporate entity which she had named as the defendant did not exist and when she later named one which did exist, without having applied for it to be substituted as defendant, she named the website owner's UK subsidiary, which was not responsible for hosting the site or for controlling what was published thereon. The master struck out her claim regarding the blog on the second website because she had also brought it against the website owner's UK subsidiary, which again was not responsible for hosting the site or for controlling what was published thereon. In the face of cases such as this one, the obligation the GDPR imposes on the controller to disclose its identity and contact details (Article 13, Article 14) may turn out to be of particular interest.

4.2.2 A second glance

In spite of the foregoing, it is here submitted that from the perspective of enhanced private enforcement the GDPR falls short of expectations. In other words, it does not provide for important elements in terms of access to the court, opportunities to litigate and/or incentives to do it:

[48] [2015] EWHC 3154 (QB). Both applications were refused. On the difficulties to identify the defendant see A. Mills, 'Suing Facebook: Vertical Private International Law Issues in Online Social Media', presentation at the Max Planck Institute Luxembourg, 16.10.2017, pending publication; K. Takahashi, 'Unmasking Anonymous Online Infringers of Personality Rights', (2015/2016) 17 Yearbook of Private International Law 181.

a. Cause of action. To start with, the Regulation does not arrange for a specific civil action regarding data protection; nor does it impose on the MS the obligation to create one.[49] In this regard the situation has not changed in comparison to the Directive, and this may have consequences in terms of obstacles to litigate. The well-known case *Google Inc. V. Vidal Hall*[50] is worth recalling here: the claimants had applied for permission to serve out of the jurisdiction for the claims for misuse of private information and for breach of confidence; the cause of action for misuse of private information is a tort for the purposes of the rules providing for service of proceedings out of the jurisdiction, thus service out of the jurisdiction is allowed; breach of confidence is not, therefore service is not allowed.

b. Limitation periods. A further left-out relates to the limitation periods for claiming compensation, which are neither harmonized nor regulated in the GDPR. The only reference thereto appears in Recital 65 and has no correspondence in the operative text: regarding the right to be forgotten, 'data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.'

c. Identification of the defendant for the purposes of the allocation of responsibility. It has just been said that the GDPR rules on the controller's duty to disclose its identity and contact details will certainly help the data subject to identify the person to be sued. However, nothing is said about the processor, who is nevertheless mentioned as a potential defendant under Article 79, and shares with the controller the liability for damages pursuant to Article 82.[51] Moreover, the category of 'controller' is still under construction and the case law much hesitant. In the aftermath of the ruling CJEU preliminary ruling in *Google Spain*,[52] the Spanish Supreme Court rendered two decisions: one by the civil senate (April 5, 2016), the other by the administrative senate (June 13, 2016); according to the latter Google Spain does not determine the purposes and means of the processing of personal data and therefore is not a controller; it is, though, according to the former. Case C-210/16 of the CJEU (*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*),[53] is worth being recalled as well in the same lines, and so is the pending case C-40/17.[54] In addition, data protection breaches may perfectly be provoked by an anonymous infringer;[55] multi-party processing operations on the internet are also likely to raise complex issues related to the identification of the (correct) defendant.[56]

d. Specific procedural track. Already before the GDPR some Member States, such as Belgium or Greece, contributed to private enforcement offering an easier access to court in the form of a special procedure. Scholars regret that the GDPR has not been taken as an occasion to fix summary proceedings before national courts for data protection violations.[57] It is worth noticing that the GDPR

[49] To be sure, in order to comply with EU law it may be sufficient for each MS to try to accommodate the already existing legal framework - although this is certainly not the best solution in terms of uniformity.

[50] Above, fn. 45.

[51] According to Articles 13 and 14 GDPR the controller shall give the contact details of its representative to the subject, but at least literally not of those of the processor. Whether Article 27.4 would allow for suing the representative in the EU in addition to or instead of the controller or processor is disputable.

[52] C- 131/12, EU:C:2014:317.

[53] ECLI:EU:C:2018:388

[54] Conclusions AG Bobek, EU:C:2018:1039.

[55] Cf. K. Takahashi (fn. 48), on the legal bases for disclosure under Japanese, French, US and English approaches.

[56] Cf. T. Wisman, 'Case Notes- Introduction: Privacy and Data Protection- Fundamentally Complex', 4 Eur. Data Prot. L. Rev. (2018) 118, 119.

[57] See A. Galetta, P. de Hert (fn. 47), 148.

suggests means to facilitate the submission of complaints to the supervisory authority -eg, providing a complaint submission form which can also be completed electronically (Article 57, Recital 141)- but not *vis-à-vis* civil actions.

e. Evidence. Regarding evidence, as explained above the opinion on a reversed burden of proof resulting from the 'accountability principle' is not unanimous. Moreover, the Regulation has not set a presumption of damage once the violation has been established: in other words, both the damages and the causality need to be proved. In addition, there is no rule on the relation between public enforcement and private follow-on actions which would allow using evidences or admissions in a prior administrative proceeding as (at least) *prima facie* evidences in a civil claim.

f. Remedies. A provision on injunctions and their scope would have been useful: an injunction adopted by the court of a Member State with a scope replicating the territorial reach of application of the GDPR (Article 3) is likely to be denied recognition and enforcement in other countries, for lack of international jurisdiction of the court of origin.

g. Costs, funding. There is nothing in the GDPR on the costs of the proceedings -contrary to other Regulations such as Regulation (EC) No 861/2007 of the European Parliament and of the Council of 11 July 2007 establishing a European Small Claims Procedure,[58] Article 16-, or regarding legal aid - like in Article 44, 45 Council Regulation (EC) No 4/2009 of 18 December 2008 on jurisdiction, applicable law, recognition and enforcement of decisions and cooperation in matters relating to maintenance obligations.[59] It may indeed be claimed that the Regulations are not comparable: the Small Claims Regulations is only about procedure in cross-border cases; the scope of the maintenance Regulation is restricted as well to cross-border situations. However, the same international nature is to be expected in many of the constellations falling under the scope of the GDPR; besides, nothing prevented the lawmaker to adopt a rule limited to cross-border cases.

g. Enforcement. Difficulties may arise linked to enforcement of a decision. On the one hand, in practice it might not be easy to make sure whether an injunction has really been complied with - in other words, to assess whether the data at stake have been removed from all possible places where they could be stored. On the other hand, the cross-border enforcement of decisions on personal data protection may be problematic, even among the EU Member States. The Proposal of the Commission included a rule on the compulsory enforcement of decisions given as a consequence of a claim *inter privatos* in intra EU cross border cases, without differentiating between injunctive or compensatory relief;[60] it did not make its way to the final text. Regarding third countries, it is worth mentioning that the decisions on defamation are currently excluded from the 'Judgments project' of The Hague Conference (the Draft Convention on the recognition and enforcement of foreign judgments in civil or commercial matters, prepared by the Special Commission of May 2018), while privacy remains between brackets. Although personal data protection is not expressly mentioned as excluded one could legitimately assume that this is the case.[61]

---

[58] OJ L 199, 31.7.2007.

[59] OJ L 7, 10.1.2009.

[60] Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Article 75.4: 'The Member States shall enforce final decisions by the courts referred to in this Article.'

[61] Cf. C. Mariottini, 'The Exclusion of Defamation and Privacy from the Scope of The Hague Draft Convention on Judgments', (2017/2018) Yearbook of Private International Law 475, 486, on an alternative to the wording currently placed in square brackets, with a specific mention to claims arising from the processing of personal data.

h. Assistance, information. The EU has clearly opted for a strong policy of data protection. In spite of it, it is fair to say that the culture of personal data protection is still underdeveloped; the idea of taking the defence of one's right in hand is alien to the EU citizens. In fields such as consumer protection the EU lawmaker has taken a proactive role imposing obligations of information to the general public and professional circles on the Member states about specific possibilities to go to court.[62] The occasion to do the same has been missed in the GDPR.

5 Conclusion

Directive 95/46/CE could not prevent legal fragmentation in the implementation of personal data protection across the Union. Its outcome in terms of private enforcement was equally poor: individuals did not find arguments persuasive enough to engage in civil judicial litigation to remedy data protection violations in the Member States.

The analysis presented earlier allows concluding that the GDPR is also a humble instrument from the point of view of private enforcement: it 'envisages and permits' both private and public enforcement,[63] while strongly privileging the latter. The same holds true for the harmonization of the rules of civil procedure in the EU - insofar as private enforcement does not play a big role the need for harmonization is limited. In this regard the field of personal data protection remains far away from other areas like damages in competition law, or IP rights.[64]

To the extent that the choice of the type of enforcement is a political one, we belief that relegating private enforcement to a discrete second place sends out the wrong signal at a crucial moment in the process of building up a culture of personal data and compliance. Cases of personal data violations before the courts, particularly against powerful controllers and processors, are largely covered by the media; in this way they contribute to raise awareness among the data subjects about the right to 'informational self-determination' and its scope. And still, under the GDPR civil court procedures remain largely unavailable. To be sure, the GDPR has opened a door to representative actions where arguments could be raised based on data protection law against the big companies in the internet business like Facebook or Google.[65] Scepticism should be allowed, though, regarding this single and, above all, incomplete provision; in particular in light of cases such as the recent *Lloyd v Google LLC*.[66]

[62] Cf. Article 24 Small Claims regulation (fn. 58).

[63] C. Hodges, 'Delivering Data Protection: Trust and Ethical Culture', 4 Eur. Data Prot. L. Rev. 65 (2018), 66.

[64] In point of truth, whether personal data protection is an area for private enforcement to work as a regulatory tool may be disputed. The reasons may be harm-related: the right to data protection can be violated without harm; when it occurs, it often pertains to the category of intangible harm, and opposed to physical damage. It is unlikely that the individual will react without harm, or an easily identifiable harm: see above, under 2.

[65] So far collective claims have usually been filed by consumer associations, based on consumer and competition law: see the cases reported by C. Etterldorf, 'Consumer Association Succeeds in First Round of Dispute Concerning Facebook's Terms of Service and Privacy Setting', 4 Eur. Data Prot. L. Rev. 114 (2018). See as well P. Rott, 'Data protection law as consumer law- How consumer organizations can contribute to the enforcement of data protection law', 2017 EuCML 113.

[66] Above fn. 37, para. 82 ff.

Max Planck Institute
LUXEMBOURG
for Procedural Law

4, rue Alphonse Weicker
L-2721 Luxembourg
www.mpi.lu