The Relationship Between Damages and Administrative Fines in the EU General Data Protection Regulation

Johanna Chamberlain* & Jane Reichel**
89 Miss. L.J. (forthcoming 2020)

1 Introduction: A New Legal Regime for Personal Data Protection in Europe

In May 2018, the new EU Data Protection Regulation, the GDPR, entered into force after a two year implementation period.¹ The two main purposes of the GDPR are to provide effective remedies for ensuring extensive personal data rights and change practices and policies of controllers and processors so that they become more aware of privacy protection. Article 58 GDPR lays down the investigative and corrective powers of the national supervisory authorities, such as issuing warnings or imposing new administrative fines. Article 79 GDPR states that every data subject whose rights according to the regulation have been infringed shall have access to an effective remedy. Such remedies typically consist of procedural tools to achieve correction, erasure etc, but also damages. The two measures in focus here are those with the largest economic impact: Article 82 on *damages* and Article 83 on *administrative fines*. These articles target different areas and subjects – while the first has a compensatory purpose and is designed for use by individuals, the second has a preventive character and is implemented by Data Protection Authorities vis-à-vis controllers and processors. Considering these two profiles, an interesting question arises: Why are the provisions of Article 83 for imposing fines on companies and organisations so detailed, while the wording of Article 82 and hence the liability for controllers and processors is open to interpretation? What does this difference lead to in the application of the regulation, and more precisely, is it likely that the development in regards to administrative fines could spill over to the application of rules on damages?

The decision to focus on sanctions and remedies within the GDPR is in itself not obvious. Traditionally, EU law has regulated substantive matters, but has left the decision on the form in which the substantive law is implemented to Member States. This division of labour between the EU and the Member States is referred to as the institutional and procedural *autonomy* of the Member

* Doctoral student in Private Law, Faculty of Law, Uppsala University, Sweden.

** Professor in Administrative Law, Faculty of Law, Stockholm University, Sweden.

¹ 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 (General Data Protection Regulation).

States.² These concepts have long been discussed in legal doctrine,³ but still need some clarification. For instance, it remains unclear what relevance the doctrine of procedural autonomy has when an EU secondary law, such as the GDPR, regulates related procedures in different manners within the same act, such as damages and administrative sanctions.

The contribution will start with a short introductory part on governance structure of data protection in EU law in relation to the principle of procedural autonomy. In the following, an analysis and comparison will be made between the two respective articles on damages and administrative fines, and their potential scope and application. The two measures will be presented and analysed in connection to their function in the respective regulatory framework – as part of the composite European administrative structure or within the procedural autonomy of the Member States. In the concluding analysis, the question is raised whether the more elaborated parameters of Article 83 may, after all, become usable within an assessment of Article 82 in the future.

2 Points of Departure: The Principle of Procedural Autonomy and its Limits

2.1 The Doctrine of Procedural Autonomy, Sanctions and Remedies

As indicated above, the realisation of EU law within the Member States has traditionally been resolved by the principle of institutional and procedural autonomy according to which the choice of institutional and procedural framework for implementation of EU law remains with the Member States. This “autonomy” is conditioned by two factors: first, it is only applicable if the EU has not enacted specific rules on the matter, and second, if the principles of effectiveness and equivalence are upheld.⁴ According to the principle of loyal cooperation in Article 4 (3) Treaty of the European Union, TEU, and the doctrine of *effet utile*, the Member States are under an obligation to make every effort to ensure that EU law is applied correctly and uniformly within each state, but how this is done precisely is for the Member States to decide.⁵ According to Article 19 TEU, it is the CJEU whose role it is to ensure that “the law is observed” in the interpretation and application of

² The principle was first established in the Case 51-54/71 *International Fruit Company v. Produktschap voor groenten en fruit* [1971] ECR, p. 1107, para. 4, and Case 33/76 *Rewe-Zentralfinanz v. Landwirtschaftskammer für das Saarland* [1976] ECR, p. 1989, para. 5. Further on, the CJEU also referred to the concept in its case law. See, for example, case C-201/02 *The Queen on the application of Wells v. Secretary of State for Transport, Local Government and the Regions* ECR 2004, p. I-723., para. 65.

³ See Kakouris, C.N., Do the Member States possess Judicial Procedural “Autonomy”?, C.M.L.Rev 34:1389-1412, 1997, p. 1404 ff.

⁴ See Case 33/76 *Rewe-Zentralfinanz v. Landwirtschaftskammer für das Saarland* EU:C:1976:188, para. 5.

⁵ Case 41/74 *van Duyn v. Home Office* EU:C:1974:133.

the treaties. The Member States, on the other hand, are to “provide remedies sufficient to ensure effective legal protection in the fields covered by Union law”. A similar division of power is often included in secondary law in relation to providing effective deterrent measures in order to maintain respect for the material EU law provisions.⁶ According to settled case law, Member States are obliged to ensure that sanctions for infringements of provisions of Union law are “effective, proportionate and dissuasive”.⁷ When applying national procedural law within the sphere of application of EU law, Member States are further obliged to uphold the general principles of EU law, as well as the EU Charter of Fundamental Rights, the Charter.⁸

One of the more significant trends in the evolution of European administrative law is that the distinction for how the doctrine of procedural autonomy applies to EU and Member State administration can no longer be upheld; the previous clear separation of duties has been superseded by forms of *administrative cooperation* between administrative bodies in the EU and its Member States.⁹ The area of data protection, with its elaborate governance structure, is a good example of this development, as discussed in the following.

2.2 The Governance Structure of EU Data Protection Law

An important aspect of the governance structure for data protection is that the independence of the authorities has been given a *constitutional denomination*.¹⁰ Both Article 16 TFEU and Article 8 of the Charter state that compliance with data protection rules shall be subject to control by an *independent authority*. Chapter VI and VII in the GDPR, Articles 51-67, regulate the independence, competence, tasks and powers of the national Data Protection Authorities, DPAs, as well as introduce mechanisms for cooperation and coherence to be applied. Further, a new EU agency has been established, the European Data Protection Board, EDPB, that has taken over the role of the previous Article 29 Data Protection Working Party (section VII, Articles 68-76).¹¹ All the DPAs are represented in the EDPB. At the Union level, Regulation 2018/1725 applies, under the supervision of a European Data Protection Supervisor, EDPS, with an equivalent legal framework

⁶ For example, Article 24 of the 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, the Data Protection Directive or DPD. See further subsection 4.2.

⁷ Case 68/88 *Commission v Greece*, EU:C:1989:339 para. 23-24 and case C-326/88, *Hansen*, EU:C:1990:291, para 17.

⁸ Joined cases C-387/02, C-391/02 and C-403/02, *Berlusconi*, EU:C:2005:270, para 67, Case C-617/10 *Åkerberg Fransson* EU:C:2013:105 and Article 51 of the Charter.

⁹ Schwarze, J, *European Administrative Law*, rev. ed. London, Sweet and Maxwell, 2006, p. cxiii.

¹⁰ Reichel, Jane & Lind, Anna-Sara, *Regulating Data Protection in the EU*, in *Perspectives on Privacy*, Dörr, Dieter & Weaver, Russell L. (Eds), de Gruyters publisher, 2014, p. 29.

¹¹ The Article 29 Working Party Group was established under Article 29 DPD.

to the national DPAs.¹² The GDPR also involves the participation of private actors. Private certification bodies, having “an appropriate level of expertise in relation to data protection”, may issue and renew certifications according to a procedure set out in Article 43 GDPR. Further, “associations and other bodies representing categories of controllers or processors” may impose a code of conduct under Articles 41–42 GDPR. Hijmans has concluded that the governance structure of EU data protection law resembles what is known in the literature as a composite administration, a multi-level governance or a multi-level stakeholder model:¹³

In short, the governance model involves roles for institutions and bodies of the European Union, Member States, National DPAs, cooperation mechanisms of DPAs, private companies and representatives of the private sector, civil society as represented by NGOs, as well as third countries and international organisations.

Two aspects of the data protection governance structure will be presented here. First, the EDPB has been tasked with issuing guidelines, recommendations, best practices and opinions on a wide range of subjects. Article 70 (1) GDPR contains a non-exhaustive list with ten areas where guidelines are to be drafted, including the setting of administrative fines pursuant to Article 83.¹⁴ This function was also carried out by the Article 29 Data Protection Working Party, although the task of the EDPB in this matter is wider and more extensively regulated in the GDPR. In October 2017, during the period when the GDPR was enacted but not yet in force, the Article 29 Data Protection Working Party issued guidelines on the application and setting of administrative fines for the purposes of the GDPR, which are discussed below.¹⁵

Secondly, the GDPR introduces several new tools through which the DPAs can cooperate, whereof two will be discussed further here: a one-stop-shop mechanism for appointing a lead authority in cases of monitoring cross-border processing in Article 56 GDPR, and a procedure for composite decision-making, labeled a consistency mechanism.¹⁶ The first mechanism allows for a smooth and foreseeable supervision since it identifies one single DPA to act as a one-stop-shop

¹² Chapter VI and VII, Articles 52-62 Regulation 2018/1725 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

¹³ Hielke Hijmans; *The European Union as a Guardian of Internet Privacy. The Story of Art 16 TEU*, Springer, 2016, p. 516-17.

¹⁴ Article 70 (1) k GDPR.

¹⁵ Article 29 Data Protection Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253)* and subsection 4.3.

¹⁶ Articles 56 and 63-66 GDPR, respectively. See further Hielke Hijmans, *The DPAs and Their Cooperation: How Far Are We in Making Enforcement of Data Protection Law More European*, 2 *Eur. Data Prot. L. Rev.* 362 (2016), p. 367-67, 369 and following.

for controllers and processors active in more than one Member State, giving the lead DPA a role as coordinator of the supervision of all the processing activities of that business throughout the EU in collaboration with other “concerned” DPAs.¹⁷

The consistency mechanism provides a procedure for fulfilling the role of a dispute resolution mechanism in which the EDPB functions as a dispute resolution body.¹⁸ According to this procedure, a DPA can refer a draft decision to the EDPB before enacting a decision in different types of situations. In the first type, in any of the six cases listed in Article 64.1,¹⁹ referral is compulsory. In the second situation, concerning “any matter of general application or producing effects in more than one Member State”, as per Article 64.2, referral is optional. However, the procedure in the second paragraph can be initiated by any DPA, not merely the one handling the matter, the lead authority, as well as the chair of the EDPB and the Commission. If the DPAs cannot agree, any one of them may trigger the consistency mechanism, thus inviting the EDPB to take a leading role. In both situations, the EDPB issues an opinion, which all DPAs and the Commission may comment on.²⁰ The lead authority must “take utmost account of the opinion of the Board” and communicate to the Chair of the Board whether it will maintain or amend its draft decision.²¹ If the lead authority does not abide by the opinion, the EDPB may proceed by enacting a dispute resolution, which is effectively a decision adopted for the individual case that the DPA must implement by enacting a final decision according to the requirements of the relevant national law, referring to the decision enacted by the EDPB.²² It is foreseen in the abovementioned guidelines that the EDPB may also enact such decisions in matters including administrative fines.²³ In case of exceptional circumstances, the GDPR further provides an urgency procedure.²⁴

¹⁷ Article 60 GDPR and Andra Giurgiu; Tine A. Larsen, Roles and Powers of National Data Protection Authorities, 2 Eur. Data Prot. L. Rev. 342 (2016), p. 349.

¹⁸ Ibid, p. 350.

¹⁹ The consistency mechanism is to be used when a DPA (a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35 (4); (b) concerns a matter pursuant to Article 40 (7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation; (c) aims to approve the requirements for accreditation of a body pursuant to Article 41 (3), of a certification body pursuant to Article 43 (3) or the criteria for certification referred to in Article 42 (5);

(d) aims to determine standard data protection clauses referred to in point (d) of Article 46 (2) and in Article 28 (8); (e) aims to authorise contractual clauses referred to in point (a) of Article 46 (3); or (f) aims to approve binding corporate rules within the meaning of Article 47.

²⁰ Article 64 (4) GDPR

²¹ Article 64 (7) GDPR. See further Recital 136 GDPR.

²² Article 65 GDPR.

²³ Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253), p. 7 and subsection 4.3.

²⁴ Article 66 GDPR.

3 Article 82: Right to Compensation and Liability

3.1 Article 82 GDPR in Extensu

Having examined the new overarching governance structure in the data protection area, it is time to have a closer look at the sanctions of the GDPR. In this section, Article 82 GDPR will be scrutinised. The wording of this article is the following:²⁵

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation.
A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.
3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.
4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.
5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.
6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79 (2).²⁶

²⁵ The entire text is included here, also below regarding Article 83, so as to make references to the many different paragraphs possible throughout the paper.

²⁶ The corresponding Recital 146 reads: “The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. 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. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.”

3.2 Differences Compared to the Data Protection Directive

In principle, the provisions for liability are the same in Article 82 as in its predecessor, Article 23 of the Data Protection Directive (DPD). The liability is often characterised as *strict*, that is, neither negligence nor willful conduct is required from the controller or processor. It suffices that the data subject can prove a breach of the regulation has occurred on the part of the controller or processor, and that this breach has resulted in eligible damages. What differentiates the so-called strict liability is the assessment of whether a breach has in fact occurred, which can be complex,²⁷ and also the fact that the controller or processor can free itself of liability if it shows that it is in no way responsible for the breach in question (Article 82.3).

One change in the wording of the article is that non-material damage is specifically mentioned as eligible for compensation. Also, according to the corresponding recital the concept of damage is to be interpreted broadly. While many Member States, Sweden for instance, interpreted the “harm” of Article 23 DPD as including both material and non-material damage, one may guess that other Member States have been stricter and demanded a connection with economic loss in order to acknowledge non-material damages. As the harm resulting from misuse of personal data is often of a non-pecuniary type, the more restrictive line would indeed have been an obstacle to the free movement of personal data within the European Union. For this reason, the clarification brought by Article 82 is a welcome change.

The other important update is the joint responsibility of the controller and processor. According to Article 23 DPD, the controller carried liability for breaches. Where a processor was in fact responsible, the data subject would still have to file a claim against the controller who, if found liable, was obliged to pay the damages and then claim the same amount from its processor. Now the system is more transparent, which makes it easier for all parties.²⁸

²⁷ For example, several of the lawful reasons for processing of personal data contain assessments of varying kinds, such as weighing the data subject’s interests against the needs and rights of other individuals (Article 6).

²⁸ See van Alsenoy, B, Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation, for a detailed survey and analysis of Article 23 DPD and Article 82 GDPR, with special focus on the “cumulative” liability between controller and processor, the burden of proof for the data subject and the possible defences for the respondents. As the author points out, the joint responsibility is in line with the principles of the harmonisation project Principles of European Tort Law (PETL). These guidelines were designed by the European Group on Tort Law and first presented in 2005.

3.3 How Should Article 82 be Interpreted by the Member States?

To date, there are no guidelines apart from the wording of the articles and their preambles regarding the interpretation of the earlier Article 23 DPD or the current Article 82 GDPR. The Article 29 Data Protection Working Party has – as mentioned above – published guidelines regarding the interpretation of Article 83 but not Article 82. The CJEU has not yet decided any cases on the application of Article 82 or, for that matter, of Article 23 DPD.

Let us therefore return to the legislation itself. We have already noted that the liability in the directly applicable Article 82 is more or less strict. It can be added that for tort law the standard causal requirement applies: damages suffered as *a result* of infringements are covered by the article. Thus, the claimant is responsible for demonstrating that the breach in question is relevant for (has caused) the harm suffered.²⁹ In summary, the first two steps in tort law – liability and causality – are basically covered by the GDPR wording.

The third step in the process of tort law – after considering the issues of liability and causality – is determining what should in fact be compensated, and how this compensation should be calculated or (in cases where exact calculation is impossible, such as with non-pecuniary damage) decided. The only help there is in Article 82 is “damages”, and in the corresponding Recital 146 “full and effective compensation”. Accordingly, all damages should be compensated in full. That is all very well and in line with the general compensatory aim of tort law, but what does it really mean? This is where national procedural autonomy comes into play, leaving the two vital questions of eligible damages and compensation levels up to the Member States – as long as the system is effective enough to ensure the impact of EU legislation. One thing that can be said is that the harm suffered must be of a kind eligible for compensation. What is acknowledged here probably varies between the European countries, but typically some substance or gravity would be required and damages would not be awarded for the general sense of unease, for example, that results from the knowledge that your personal information is “out there”. The levels of compensation without doubt vary considerably depending on the legal order and are constantly evolving.

²⁹ Divergence from this typically consists of different forms of softer causality requirements. For example, in Sweden, when there are several potential reasons or chains of events for an occurred harm the court will often accept the reason that is deemed most “predominantly likely”. However, when it comes to non-pecuniary damage, it is usually difficult to “show” a concrete harm. In these cases, harm can be said to be presumed as long as a relevant breaching action has been established. Thus, the requirements on the injured party when it comes to proven harm and causality can become difficult to separate in these cases. Non-pecuniary damages are, as mentioned above, the typical kind of damage resulting from GDPR breaches.

The Member States are left with the question of how far the national flexibility can be supposed to stretch in the data protection area. How extensive can the interpretation of compensable harms be, and how high can damages awarded be, without creating a risk of conflict with the Internal Market and the principle of free movement for personal data within the Union? How low can they be, and how restrictive can the interpretation of compensable harms be, while still complying with the victim's right to full compensation and an effective remedy (Article 79 GDPR)? Considering this unclear state of affairs, the possibility to draw some inspiration from the detailed factors of Article 83 should definitely be of interest. These parameters, and the guidelines for interpreting them, will be examined in the following.

4 Article 83: General Conditions for Imposing Administrative Fines

4.1 Article 83 in Extensu

The wording of (the extensive) Article 83 GDPR is as follows:

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) or Article 58 (2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
 - (a) the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
 - (b) the intentional or negligent character of the infringement;
 - (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
 - (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
 - (e) any relevant previous infringements by the controller or processor;
 - (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
 - (g) the categories of personal data affected by the infringement;
 - (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
 - (i) where measures referred to in Article 58 (2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
 - (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
 - (k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.
4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:
 - (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
 - (b) the obligations of the certification body pursuant to Articles 42 and 43;
 - (c) the obligations of the monitoring body pursuant to Article 41 (4).
5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:
 - (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
 - (b) the data subjects' rights pursuant to Articles 12 to 22;
 - (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
 - (d) any obligations pursuant to Member State law adopted under Chapter IX;
 - (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58 (2) or failure to provide access in violation of Article 58 (1).
6. Non-compliance with an order by the supervisory authority as referred to in Article 58 (2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58 (2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.
8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.
9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.³⁰

³⁰ The corresponding Recital 148, which does not really add much to the parameters formulated in Article 83 (2), reads: "In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or

4.2 Changes since the Data Protection Directive

In comparison with the DPD, the GDPR has introduced fines. In the Directive, it was merely stated that “(t)he Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive”.³¹ This did not have to include administrative fines, and in the abovementioned Guidelines enacted by the Article 29 Data Protection Working Party it is acknowledged that “fining powers represent for some national supervisory authorities a novelty in the field of data protection, raising numerous issues in terms of resources, organization and procedure”.³² In line with the recitals, especially number 148, the administrative fines have been introduced as a penalty to complement the earlier measures and strengthen the enforcement of the GDPR principles. Thus, the aim of Article 83 is preventive – to deter companies and other actors from breaching the data protection rules.

In Denmark and Estonia, the regulatory regime with administrative fines issued by an authority was deemed contrary to the legal system, which necessitated these two states to organise their rules differently. In the recitals it is declared that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities.³³

In the Article 29 Data Protection Working Party Guidelines on administrative fines, which are the focus of the next subsection, it is emphasised that the decision to fine someone will be appealable, presumably referring to future case law from national courts and the CJEU.³⁴ As of now, however, it can be held that the realisation of the aim proclaimed in Recital 10 of the GDPR – that the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States – remains a work in progress. In this context, any

mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.”

³¹ Article 24 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.

³² Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253), p. 8.

³³ Recital 151.

³⁴ Ibid.

guidance that the DPAs may be able to procure is valuable. The guidelines can, in spite of their non-binding character, be expected to become quite influential.

4.3 A Common Understanding – The Article 29 Data Protection Working Party Guidelines

The Article 29 Data Protection Working Party published guidelines regarding the interpretation of Article 83 in October 2017. These are intended for use by the supervisory authorities to ensure an effective enforcement of the GDPR and reflect a common understanding of the assessment criteria in Article 83 (2).³⁵

When an infringement of the Regulation has been established, the first step for the national supervisory authority is to assess which corrective measure should be used. Administrative fines are not the only option; the abovementioned Article 58 offers a number of different measures. The supervisory authority can issue warnings, reprimands or orders, and withdraw certifications, as well as imposing fines.³⁶ All corrective measures should “adequately respond to the nature, gravity and consequences of the breach”, and the authorities must “assess all the facts of the case in a manner that is consistent and objectively justified” to find a corrective measure that is “effective, proportionate and dissuasive in each case”.³⁷ The objective of these measures can be either to reestablish compliance with rules, punish unlawful behaviour, or both. The meaning of the broad terms *effective*, *proportionate* and *dissuasive* is to be determined by the supervisory authorities and the CJEU in the years to come. The Article 29 Data Protection Working Party has highlighted the fact that the administrative fines should not be seen as a “last resort”, but should instead be used effectively.³⁸

It can be noted that Article 83 provides for a two-tiered system, explicitly stating that some violations are more severe than others. The first tier includes violation of articles governing the responsibilities of different actors (controllers, processors, certification bodies, etc.) and may result in a fine of up to € 10 million, or 2% of the firm’s worldwide annual revenue from the preceding financial year, whichever amount is higher.³⁹ The second tier includes violations of individual rights protected by the GDPR, such as the basic principles for processing, the data subjects’ rights to

³⁵ Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253) p 4.

³⁶ See on this assessment the above-mentioned Recital 148.

³⁷ Article 29 Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253) p 6.

³⁸ Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253) p 7.

³⁹ Article 83 (4) GDPR.

information, transfer rules, etc. These types of infringements could result in a fine of up to € 20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.⁴⁰ In both tiers, there are two assessments to be conducted: whether a fine should be imposed, and the amount of the fine. In both assessments all individual factors are to be considered based on the same parameters given in Article 83 (2). However, the conclusions reached in the first step may be directly used in the second step if such an approach means avoiding having to make the same assessment twice.⁴¹ The Data Protection Working Party document provides guidelines on how to interpret the various factors given in Article 83 (2) above when making the two assessments.

Even if it is first and foremost a question for the DPA to make the assessment in the individual case, the coherence mechanism remains available. The guidelines further foresee that the EDPB may make use of its competence in Article 65 to enact a decision within the dispute resolution:⁴²

The EDPB, when competent according to article 65 of the Regulation, will issue a binding decision on disputes between authorities relating in particular to the determination of the existence of an infringement. When the relevant and reasoned objection raises the issue of the compliance of the corrective measure with the GDPR, the decision of EDPB will also discuss how the principles of effectiveness, proportionality and deterrence are observed in the administrative fine proposed in the draft decision of the competent supervisory authority.

It is also predicted that the EDPB will give guidance on the application of Article 65 GDPR for further details on the type of decision to be taken by the EDPB.⁴³

5 Sanctions and Remedies under the GDPR – Composite or National?

5.1 Defining the Procedural Context for GDPR Sanctions and Remedies

⁴⁰ See further on the two-tiered system, Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253) p 9.

⁴¹ Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253) p 9.

⁴² Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253) p 7.

⁴³ Ibid.

Before the GDPR entered into force, the lack of harmonisation of national implementation laws had led to a high degree of diversity in regards to the regulation of sanctions.⁴⁴ With the GDPR, the conditions have, as noted, changed; the DPAs are now expected to cooperate with each other and with the EDPB in their application of the GDPR provisions. With regard to damages, no equivalent actor, competent authority or similar, has been tasked with its implementation. There is accordingly a manifest difference in approach between the two measures discussed here – damages and administrative fines. Where Article 83 GDPR is to be handled by all the DPAs in a consistent manner, the Member States have freedom in relation to Article 82 when it comes to deciding what bases and levels of compensation for damages are appropriate. The consequences of both approaches are discussed below.

5.2 GDPR Sanctions as part of a European Composite Administration

As already concluded above, the governance structure for EU data protection law has been defined as a composite administration, a multi-level governance or a multi-level stakeholder model.⁴⁵ The regulation of administrative fines is a central part of this governance structure, where the DPAs are to apply the sanctions in an equivalent manner under the guidance of the EDPB and, if relevant, after having followed the procedures of the coherence mechanism. On the other hand, even though Article 83 GDPR is extensive in its wording, it cannot be considered an exhaustive regulation of the DPA's functions and responsibilities when handling matters of administrative fines. There are still lacunas to be filled by national law, for example, administrative safeguards connected to handling matters, such as the duty to investigate diligently, the right to be heard of the parties involved, the obligation to reason decisions, and so forth. The guidelines further acknowledge that national law may include additional requirements on the enforcement procedure, for example, address notifications, form, deadlines for making representations, appeal, enforcement and payment.⁴⁶ As mentioned above, Denmark and Estonia have organised their regime for fining differently than the others due to national legal constraints.⁴⁷

Member States are obliged to uphold the general principles of EU law and the Charter when acting within the sphere of EU law, as discussed above. According to case law, the obligation includes

⁴⁴ Andra Giurgiu & Tine A. Larsen, *Roles and Powers of National Data Protection Authorities*, 2 *Eur. Data Prot. L. Rev.* 342 (2016), p. 344.

⁴⁵ Hielke Hijmans; *The European Union as a Guardian of Internet Privacy. The Story of Art 16 TEU*, Springer, 2016, p. 516-17 and above subsection 2.2.

⁴⁶ Article 29 Data Protection Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253)* p 6.

⁴⁷ Recital 151 GDPR and subsection 2.2.

the right to good administration, for example, the abovementioned procedural safeguards of duty to investigate diligently, etc.⁴⁸ This does not necessarily exclude the application of national administrative procedural law since the EU general principles and Charter often function as a minimum protection. As the CJEU held in the *Åkerberg Fransson* case, national authorities and courts may apply national standards “provided that the level of protection provided for by the Charter, as interpreted by the Court, and the primacy, unity and effectiveness of European Union law, are not thereby compromised”.⁴⁹ In areas that are comprehensively regulated by EU law, the CJEU has, however, held that the national courts are obliged to follow the EU standard in full, for example, in cases of repayment of agricultural subsidies.⁵⁰ In the GDPR, the question of what standard of protection the DPAs are to uphold when handling matters on sanctions is depicted in a way that can be described as fluid or fuzzy. In the recitals, reference is only made to EU law:⁵¹

The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

In Article 58 (4) GDPR, where the DPA’s powers are listed, reference is made to EU and national law “in accordance with the Charter”:

The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

Lastly, in Article 83 (8) GDPR, where the administrative fines are regulated, reference is made to EU law and national law as two independent sources:

The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

⁴⁸ Case C-604/12 *H. N. v. Minister for Justice, Equality and Law Reform*, EU:C:2014:302, p. 49–50 and C 46/16, *Valsts ieņēmumu dienests mot “LS Customs Services”* SIA, EU:C:2017:839, p. 46.

⁴⁹ Case C-617/10 *Åklagaren v. Åkerberg Fransson*, EU:C:2013:280, p. 29.

⁵⁰ C-568/11 *Agroferm*, EU:C:2013:407, p. 51.

⁵¹ Recital 148 GDPR.

It must be said that it is unfortunate that the GDPR in itself includes three different wordings on such a central issue. The guidelines do not include any further information on the matter. It remains unclear whether procedural safeguards are included in the area of law that is to be applied in a coherent manner or if national procedural autonomy remains relevant.

5.3 GDPR Remedies as part of National Law

When applying GDPR rules on damages, the situation is different. EU law does not contain an equivalent regulatory regime to apply at the national level, whereby the main rule of national procedural autonomy can be excepted to play a more decisive role than in relation to administrative sanctions. EU procedural law will thus only be relevant if national law does not fulfil the requirements of efficiency and equivalence.⁵²

In the introduction, the question was raised whether it is likely that the development in regards to administrative fines could spill over to the application of rules on damages. In order to analyse this issue further, a relevant question to investigate is what is meant by the requirement that national procedural law is applied in an equivalent manner. Do high administrative fines for a certain category of violations mean that damages on the same category should also be high?

In analysing the case law of the CJEU on the principle of equivalence, the answer to this question is presumably to be answered in the negative. The principle only means that actions based on EU law are to be treated equivalently to similar actions based on national law. What is defined as “similar actions” should be based on an analysis of the kind of legal action at stake. The fact that national procedural law provides for better conditions in proceedings of a different nature, or is applicable to proceedings falling within two different branches of law, is not contrary to the principle of equivalence.⁵³ In the *Dragos* case, the applicant chose to proceed with a civil law suit instead of an administrative procedure for reimbursement of administrative fees collected in violation of EU law. The latter, but not the former, provided a mechanism for revising a final decision. The CJEU held that:⁵⁴

It follows that the principle of equivalence does not preclude a situation where there is no possibility for a national court to revise a final decision of a court or tribunal made in the

⁵² See above subsection 2.1.

⁵³ Case C-200/14, *Câmpean*, EU:C:2016:494, p. 55-56.

⁵⁴ Case C-69/14, *Dragoș Constantin Târșia v. Statul român*, EU:C:2015:662, p. 35.

course of civil proceedings when that decision is found to be incompatible with an interpretation of EU law upheld by the Court after the date on which that decision became final, even though such a possibility does exist as regards final decisions of a court or tribunal incompatible with EU law made in the course of administrative proceedings.

If remedies of an administrative nature are found to belong to a different branch of law to remedies of a civil law nature, the two are not to be considered “similar actions” in relation to the principle of equivalence. Based on this line of reasoning, the doctrine of procedural autonomy does allow Member States to uphold stricter conditions and less beneficial procedural rules in relation to actions for damages for transgressions of the GDPR than for administrative sanctions for the same type of transgression. The question remains whether these differences in remedies for breaches of data protection law may cause inconsistencies in internal national law in such a manner that the Member States may find it better to adjust voluntarily. This question will be analysed in the following final section.

6 Conclusive Analysis: Is there a Potential Bridge between Article 82 and Article 83 GDPR?

The practice of referring questions of sanctions to national law under the doctrine of procedural autonomy can be explained by the reluctance displayed by the Member States to hand over their sanctioning powers to the EU.⁵⁵ By leaving the matter of regulating administrative sanctions to the Member States, national sanctions can be applied under one comprehensive set of rules, within the legal system of the Member State.

In the GDPR, sanctions and damages are regulated in different ways. While administrative fines are regulated in a (at least potentially) composite manner, damages are regulated according to national law under the doctrine of procedural autonomy. Thus, the regulatory regime for sanctions under the GDPR does seem to have contradictory effects on national law: The administrative governance structures analysed in subsection 5.1 are moving national sanction law on administrative fines towards an integrated European process with the potential effect of diminishing the internal coherence of national law. Administrative fines based on the GDPR are to be applied in a European manner, which may deviate from how administrative fines are applied in other sector specific areas within the same Member State. The conclusions of the case law presented in subsection 5.2, on the other hand, isolate the European influences from national law

⁵⁵ de Moor-van Vugt, A. Administrative sanctions in EU law, in Jansen, Oswald, Administrative Sanctions in the European Union, Intersentia 2013, p. 608.

on damages and only cause disruptions to the coherence of national law in cases where actions based on national law are to be given a more beneficial treatment. EU law does not require total Europeanisation of remedies applicable to EU matters, but only that they are effective and non-discriminatory. This situation should be rather easy to avoid and damages based on the GDPR can remain embedded in national law.

Can this dual approach be upheld? Or will the mechanisms for achieving coherency within the administrative structure regarding administrative fines spill over on damages? According to Article 83 (2)(a), due regard shall be given to the nature, gravity and duration of the infringement, as well as the number of data subjects affected and the level of damage suffered by them. Here is an explicit connection to damages (supposedly non-material as well as material) and the rights and freedoms of natural persons. In the corresponding section of the Working Party Guidelines, under “Nature, gravity and duration of infringement”, the occurrence of damage to data subjects is mentioned. The level of such damage is to be considered within the Article 83 assessment of which corrective measure to select.⁵⁶ This can be compared to the statement in Recital 148 that “actions taken to mitigate the damage suffered” should be considered within the assessment of imposing fines. Thereby, it is clear that the compensatory principles of Article 82 have an impact on the imposition of administrative fines, according to the Working Paper Guidelines and recital – if not on deciding the amount, which is curious as the wording of Article 82 (3) includes both steps of the assessment.

Could the parameters in Article 83 (2) be seen as relevant for a damages assessment according to Article 82? It should be made clear that the GDPR contains no indication that inspiration can be drawn in this way, but at the same time the flexibility of Article 82 does not argue against it either. The guidelines on Article 83 simply say they provide no explanation of the differences between administrative, civil or criminal law systems when imposing administrative sanctions in general.⁵⁷

As a tentative approach, a guiding principle could be that factors in Article 83 (2) connected to the *data subject*, such as (a) and (g), are highly relevant for Article 82. Further, factors connected to the *harmful act* itself and thus the controller or processor: (b), (c), possibly also (d), (e) and (f), could be seen as relevant. Assessment criteria that are more closely connected to the *supervisory authorities* and

⁵⁶ Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253) p 11.

⁵⁷ Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253) p 4.

the corrective measures of the GDPR: (h), (i) and (j) are far from the compensatory purpose and the focus on the data subject of Article 82, and should therefore not be taken into account under Article 82. They belong within the preventive aim of Article 83. The last criteria, (k), referring to “any other aggravating or mitigating factor” could of course always be of relevance depending on the individual case.

For national data protection law, the possible convergence between EU administrative fines and damages for breaches of the GDPR could have a beneficial effect on the internal coherence of this particular area of law. It could be seen as unreasonable that a data subject having had his or her data privacy breached is awarded nothing or a relatively small sum in damages, while the DPA issues an administrative fine in the second tier of Article 83 GDPR, which may be quite high. From a broader perspective, this may however lead to at least two uncertainties. First, what happens to the internal coherence of the national legal orders of the Member States – for instance, the relationship with other non-pecuniary damages – if the law on sanctions and remedies for breaches of data protection becomes increasingly Europeanised? Second, if or when the law on sanctions and remedies for breaches of data protection law does become increasingly Europeanised, who is ultimately in charge of monitoring that appropriate procedural safeguards, such as the duty to investigate diligently, the right to be heard of the parties involved and effective judicial remedies, are upheld within the composite structure? Only the future will tell.