THE RELATIONSHIP BETWEEN DAMAGES AND ADMINISTRATIVE FINES IN THE EU GENERAL DATA PROTECTION REGULATION

Johanna Chamberlain[*] *& Jane Reichel*[**]

[*] Doctoral student in Private Law, Faculty of Law, Uppsala University, Sweden.
[**] Professor in Administrative Law, Faculty of Law, Stockholm University, Sweden.

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.[2] Article 58 of the GDPR lays out the investigative[3] and corrective[4] powers of the national supervisory authorities, such as issuing warnings or imposing new administrative fines. Article 79 of the GDPR states that every data subject whose rights according to the regulation have been infringed shall have access to an effective remedy.[5] Such remedies typically consist of procedural tools to achieve correction, erasure, etc.,[6] but also include damages.[7]

The two measures in focus here are those with the largest economic impact: (1) Article 82 on *damages*, and (2) 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 ("DPAs") *vis-á-vis* controllers and processors. Considering these two

---

[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), 2016 O.J. (L 119), https://eur-lex.europa.eu/eli/reg/2016/679/oj [hereinafter GDPR] [https://perma.cc/A3TP-EP5B].

[2] *Id.* art. 4.

[3] *Id.* art. 58(1).

[4] *Id.* art. 58(2).

[5] *Id.* art. 79(1) ("[E]ach data subject shall have the right to an effective judicial remedy.").

[6] *Id.* art. 13(2)(b).

[7] *Id.* arts. 82, 83.

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 GDPR's sophistication 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 enforced to Member States under the doctrine of *institutional* and *procedural autonomy*.[8] These concepts have long been discussed in legal doctrine,[9] 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.[10]

This Article will, first, provide a short introductory on governance structure of data protection in EU law in relation to the principle of procedural autonomy. Second, 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 functions in the respective regulatory framework—as part of the composite European administrative structure or within the procedural autonomy of the Member States. Third, and in conclusion, this Article analyses the question of whether the more elaborate parameters of Article 83 may, after all, become usable within an assessment of Article 82 in the future.

---

[8] The principle was first established in Case 51/71, Int'l Fruit Co NV v. Produktschap voor groenten en fruit, 1971 E.C.R. 1107, ¶ 4, and Case 33/76, Rewe-Zentralfinanz v. Landwirtshaftskammer für das Saarland, 1976 E.C.R. 1989, ¶ 5. Further on, the Court of Justice of the European Union also referred to the concept in its case law. *See, e.g.*, Case C-201/02, The Queen on the application of Wells v. Secretary of State for Transport, Local Government and the Regions, 2004 E.C.R. I-723, ¶ 65.

[9] *See* C.N. Kakouris, *Do the Member States Possess Judicial Procedural "Autonomy"?*, 34 COMMON MKT. L. REV. 1389, 1404 (1997).

[10] *See* GDPR, *supra* note 1, art. 82, 83.

I. POINTS OF DEPARTURE: THE PRINCIPLE OF PROCEDURAL AUTONOMY AND ITS LIMITS

A. The Doctrine of Procedural Autonomy, Sanctions and Remedies

As indicated above, the realization of EU law within the Member States has traditionally been resolved by the principle of institutional and procedural autonomy, under which choices in the enforcement of EU law remains with the Member States.[11] This "autonomy" is conditioned by two factors: first, it applies only if the EU has not enacted specific rules on the matter, and second, it applies only if the principles of effectiveness and equivalence are upheld.[12] According to the principle of loyal cooperation in Article 4(3) of the Treaty on European Union ("TEU"),[13] 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 is precisely for the Member States to decide.[14] According to Article 19 of the TEU, it is the Court of Justice of the European Union whose role it is to ensure that "the law is observed" in the interpretation and application of the treaties.[15] The Member States, on the other hand, are to "provide remedies sufficient to ensure effective legal protection in the fields covered by Union law."[16] 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

---

[11] Kakouris, *supra* note 9, at 1404.

[12] *See* Rewe-Zentralfinanz v. Landwirtshaftskammer für das Saarland, 1976 E.C.R. 1989, ¶ 5 ("[I]n the absence of Community rules on this subject, it is for the domestic legal system of each Member State to designate the courts having jurisdiction and to determine the procedural conditions governing actions at law intended to ensure the protection of the rights which citizens have from the direct effect of Community law, it being understood that such conditions cannot be less favourable than those relating to similar actions of a domestic nature.").

[13] *See* Consolidated version of the Treaty on European Union art. 4(3), Oct. 26, 2012, 2012 O.J. (C 326), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012M%2FTXT [hereinafter TEU] [https://perma.cc/8EUU-VQP6].

[14] *See* Case 41/74, van Duyn v. Home Office, 1974 E.C.R. 1337.

[15] *See* TEU, *supra* note 13, art. 19(1).

[16] *See id.*

EU law provisions.[17] According to settled case law, Member States are obliged to ensure that sanctions for infringements of provisions of EU law are "effective, proportionate and dissuasive."[18] 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.[19]

One of the more significant trends in the evolution of European administrative law is that there is no longer a distinction between EU and Member State administrations in terms of how the doctrine of procedural autonomy applies. The previous clear separation of duties has been superseded by forms of *administrative cooperation* between administrative bodies in the EU and its Member States.[20] The area of data protection, with its elaborate governance structure, is a good example of this development, as discussed in the following section.

B. 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*."[21] Both Article 16 of the Treaty of the Functioning of the European Union ("TFEU")[22] and

---

[17] *See, e.g.*, 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, art. 24, 1995 O.J. (L 281/31), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 [hereinafter Data Protection Directive] [https://perma.cc/QB8X-BYSY] (repealed by GDPR, *supra* note 1); *see also infra* Part III(*B*).

[18] Case C-326-88, Anklagemyndigheden v. Hansen & Soen I/S, 1990 E.C.R. I-02911, ¶ 17; *see also* Case 68/88, Comm'n v. *Hellenic Republic*, 1989 E.C.R. 2965, ¶¶ 23-24.

[19] Case C-617/10, Åklagaren v. Åkerberg Fransson, 2013 E.C.R. 00000, ¶ 29; Joined Cases C-387/02, C-391/02 & C-403/02, 2005 E.C.R. I-03565, ¶ 67; *see also* Charter of Fundamental Rights of the European Union art. 51, 2000 O.J. (C 364), https://www.europarl.europa.eu/charter/pdf/text_en.pdf [hereinafter Charter] [https://perma.cc/CA23-PA2U].

[20] JÜRGEN SCHWARZE, EUROPEAN ADMINISTRATIVE LAW cxiii (rev. 1st ed. 2006).

[21] Jane Reichel & Anna-Sara Lind, *Regulating Data Protection within the European Union*, *in* PERSPECTIVES ON PRIVACY: INCREASING REGULATION IN THE USA, CANADA, AUSTRALIA, AND EUROPEAN COUNTRIES 22, 29 (Dieter Dörr & Russell L. Weaver eds., 2014) (emphasis added).

[22] Consolidated Version of the Treaty on the Functioning of the European Union art. 16, Oct. 26, 2012, 2012 O.J. (C 326), https://eur-lex.europa.eu/legal-

Article 8 of the Charter[23] state that compliance with data protection rules shall be subject to control by an *independent authority*. Chapters VI and VII in the GDPR, Articles 51-67, regulate the independence, competence, tasks and powers of the national DPAs, as well as introduce mechanisms for cooperation and coherence.[24] Further, under Articles 68-76 in the GDPR, a new EU agency has been established, the European Data Protection Board ("EDPB"), which has taken over the role of the Data Protection Directive's Article 29 Data Protection Working Party.[25] 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 to the national DPAs.[26] 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 of the GDPR.[27] Further, "associations and other bodies representing categories of controllers or processors" may impose a code of conduct under Article 40(2) of the GDPR, subject to Articles 41 and 42.[28] Hielke 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."[29]

---

content/EN/TXT/?uri=celex%3A12012E%2FTXT [hereinafter TFEU] ("Compliance with these rules shall be subject to the control of independent authorities.") [https://perma.cc/8TFK-Z8RX].

[23] Charter, *supra* note 19, art. 8(3) ("Compliance with these rules shall be subject to control by an independent authority.").

[24] GDPR, *supra* note 1, arts. 51-67.

[25] *Id.* arts. 68-76. The Article 29 Data Protection Working Party Group was established under the Article 29 of the Data Protection Directive. *See* Data Protection Directive, *supra* note 17, art. 29.

[26] *See* Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC art. 1(3), 2018 O.J. (L 295/39), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725 [https://perma.cc/J9V2-XW3A].

[27] GDPR, *supra* note 1, art. 43.

[28] *Id.* art. 40; *see also id.* arts. 41-42.

[29] HIELKE HIJMANS, THE EUROPEAN UNION AS GUARDIAN OF INTERNET PRIVACY: THE STORY OF ART 16 TFEU 517 (2016).

> 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.[30]

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.[31] Article 70(1) of the 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.[32] 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.[33] 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.[34]

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 of the GDPR, and a procedure for composite decision-making, labeled a "consistency mechanism."[35] Because it identifies one single DPA to act as a one-stop-shop for controllers and processors active in more than one Member State, the first mechanism allows for a smooth and foreseeable supervision, making the lead DPA the

---

[30] *Id.* at 516.

[31] GDPR, *supra* note 1, art. 70(1)(d), (f)-(k).

[32] *Id.*

[33] *See* Data Protection Directive, *supra* note 17, arts. 29-30.

[34] *See* Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (Oct. 3, 2017), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237 [hereinafter Article 29 Data Protection Working Party Guidelines] [https://perma.cc/S3TD-FXZU]; *see also infra* Part III(*C*).

[35] *See* Hielke Hijmans, *The DPAs and Their Cooperation: How Far Are We in Making Enforcement of Data Protection Law More European?*, 2 EUR. DATA PROTECTION L. REV. 362, 367-72 (2016) (discussing the "one stop shop mechanism" and the "consistency mechanism"); *see also* GDPR, *supra* note 1, arts. 56, 63-66.

coordinator of supervision of all processing activities of that business throughout the EU in collaboration with other "concerned" DPAs.[36]

The consistency mechanism provides a procedure for "fulfill[ing] the role of a dispute resolution mechanism, in which the EDPB functions as a dispute resolution body."[37] Under this procedure, a DPA can "submit a draft decision to the EDPB"[38] before enacting a decision in different types of situations. In the first type, in any of the six cases listed in Article 64(1), referral is compulsory.[39] In the second situation, concerning "any matter of general application or producing effects in more than one Member State," under Article 64(2), referral is optional.[40] However, the

---

[36] *See* Andra Giurgiu & Tine A. Larsen, *Roles and Powers of National Data Protection Authorities*, 2 EUR. DATA PROTECTION L. REV. 342, 349 (2016) ("Under the new one-stop-shop mechanism, the lead DPA will coordinate the supervision of all the processing activities of that business throughout the EU, in collaboration with other concerned DPAs." (footnotes and internal quotation marks omitted)); Hijmans, *supra* note 35, at 367 ("Where the processing of personal data takes place in more than one Member State, one single DPA should act as a one stop shop for controllers and processors.)); *see also* GDPR, *supra* note 1, arts. 60, 63.

[37] Giurgiu & Larsen, *supra* note 36, at 350.

[38] *Id.*

[39] *See* GDPR, *supra* note 1, art. 64(1). Article 64(1) provides:

> (1) The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:
>
> (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 criteria for accreditation of a body pursuant to Article 41(3) of a certification body pursuant to Article 43(3);
>
> (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.

Id.

[40] *Id.* art. 64(2).

procedure in the Article 64(2) can be initiated by any DPA, not merely the lead authority handling the matter, as well as the chair of the EDPB and the Commission or "any supervisory authority."[41] If the DPAs cannot agree, any one of them may trigger the consistency mechanism, thus inviting the EDPB to take a leading role.[42] In both situations, the EDPB issues an opinion, on which all DPAs and the Commission may comment.[43] 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.[44] 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.[45] It is foreseen in the abovementioned Article 29 Working Party Guidelines that the EDPB may also enact such decisions in matters including administrative fines.[46] In case of exceptional circumstances, the GDPR further provides an urgency procedure.[47]

II. ARTICLE 82: RIGHT TO COMPENSATION AND LIABILITY

A. Article 82 GDPR

Having examined the new overarching governance structure of data protection, this Article will now examine and scrutinize the sanctions of the GDPR. In particular, Article 82 of the GDPR provides:

---

[41] *Id.*

[42] *Id.*

[43] *Id.* arts. 64(2), (3).

[44] *Id.* art. 64(7); *see also id.* ¶ 136.

[45] *Id.* art. 65.

[46] Article 29 Data Protection Working Party Guidelines, *supra* note 35, at 7 ("When the relevant and reasoned objected raises the issue of compliance of the corrective measure with the GDPR, the decision of the 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."); *see also infra* Section III(*C*).

[47] GDPR, *supra* note 1, art. 66.

(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 involves 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).[48]

---

[48] *Id.* art. 82. The corresponding Recital 146 provides:

The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The

B. 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).[49] Liability under both can be characterised as *strict*, meaning neither negligence nor willful conduct is required from the controller or processor.[50] 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.[51] What differentiates the so-called strict liability between the Data Protection Directive and the GDPR is the assessment of whether a breach has in fact occurred, which can be complex,[52] and

> 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.

Id. ¶ 146.

[49] Data Protection Directive, *supra* note 17, art. 23.

[50] Brendan Van Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, 7 J. OF INTELL. PROP., INFO. TECH. AND E-COM. L. 271, 273 (2016) ("The liability rule of [A]rticle 23 [of the Data Protection Directive] has been characterized as a form of 'strict' (i.e. 'no fault') liability."); *id.* at 282 ("The liability regime for controllers has remained 'strict' under the GDPR . . . .").

[51] *Id.* at 282 ("[O]nce an infringement has been established, the controller cannot escape liability simply by demonstrating the absence of personal fault. The controller shall therefore remain liable for unlawful processing activities undertaken by the processor on its behalf, even if the controller were to demonstrate an absence of fault in either his choice or supervision of the processor." (footnote omitted)).

[52] 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. *See* GDPR, *supra* note 1, art. 6(1).

also the fact that, under the GDPR, the controller or processor can free itself of liability if it shows that it is in no way responsible for the breach in question.[53]

One change in the wording of Article 82 is that "non-material damage" is specifically mentioned as eligible for compensation.[54] Also, according to corresponding Recital 146, the concept of damage is to be "broadly interpreted."[55] While many Member States, like Sweden, for instance, interpreted the "harm" of Article 23 of the Data Protection Directive as including both material and non-material damage,[56] 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.[57]

The other important update is the joint responsibility of the controller and processor. According to Article 23 of the Data Protection Directive, the controller carried liability for breaches.[58] 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.[59]

---

[53] *Id.* art. 82(3).

[54] *Id.* art. 82(1).

[55] *Id.* ¶ 146.

[56] § 14 Government Bill 1997/98:44 (Prop. 1998/98:44) (Swed.).

[57] *See* Van Alsenoy, *supra* note 50, at 284 ("While [the right to non-pecuniary damages] was arguably already the case under Directive 95/46, the clarification is nevertheless welcome with a view of removing doubt and ensuring a harmonised approach among EU member states.").

[58] Data Protection Directive, *supra* note 17, art. 23.

[59] For a detailed survey and analysis of Article 23 of the Data Protection Directive and Article 82 of the GDPR, see Van Alsenoy, *supra* note 50, at 282 (contrasting the GDPR as providing "a 'cumulative' liability regime, whereby each act can be held liable in light of its role in the processing"). Van Alsenoy also analyses the burden of proof in GDPR damage claims, as well as possible defences for the respondents. *See id.* at 282-84. As Van Alsenoy points out, "[t]he cumulative liability regime of [A]rticle 82(4) of the GDPR reflects the Principles of European Tort Law (PETL)." *Id.* at 286; *see also*

C. 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 of the Data Protection Directive or the current Article 82 of the GDPR. The Article 29 Data Protection Working Party has, as mentioned above, published guidelines regarding the interpretation of Article 83, but not for Article 82.[60] The Court of Justice of the European Union has not yet decided any cases on the application of Article 82 or, for that matter, Article 23 of the Data Protection Directive.

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 Article 82.[61] Thus, the claimant is responsible for demonstrating that the breach in question is relevant for, or has caused, the harm suffered.[62] In summary, the first two steps in European tort law—liability and causality—are inherent in the GDPR's 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 those with non-pecuniary damages) decided. The only help existing in Article 82 is the word "damages," and in the corresponding Recital

---

PRINCIPLES OF EUROPEAN TORT LAW: TEXT AND COMMENTARY (Eur. Grp. On Tort Law 2005).

[60] *See* Article 29 Data Protection Working Party Guidelines, *supra* note 34.

[61] See GDPR, *supra* note 1, art. 82(1) ("as a result of an infringement").

[62] 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. *See* JAN HELLNER & MARCUS RADETZKI, SKADESTÅNDSRÄTT 193 (2018) (Swed.) (Tort Law); HÅKAN ANDERSSON, SKYDDÄNDAMÅL OCH ADEKVANS: OM SKADESTÅNDSANSVARETS GRÄNSER 60 (1993) (Swed.) (The Limits of Liability in Tort Law).

146 the phrase "full and effective compensation."[63] 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. This determination 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, harm which results from the knowledge that your personal information is "out there" falls into this category. The levels of compensation therefore, without doubt, vary considerably depending on the legal order and are constantly evolving.

As a result of provided discretion, the Member States are left with the question of how far national flexibility can stretch in the realm of data protection. How extensive can the interpretation of compensable harms be, and how high can damages awarded be, without creating a risk of conflict with the fundamental EU aim of establishing an Internal Market connecting the 27 domestic markets of the Member States,[64] and the principle of free movement for personal data within this market? 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 the "effective judicial remedy" requirement?[65] 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 section.

---

[63] *See* GDPR, *supra* note 1, art. 82; *id.* ¶ 146.

[64] *See* TFEU, *supra* note 22, art. 26.

[65] *See* GDPR, *supra* note 1, art. 79.

III. ARTICLE 83: GENERAL CONDITIONS FOR IMPOSING ADMINISTRATIVE FINES

A. Article 83

The extensive Article 83 of the GDPR provides:

> (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) of 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.[66]

B. Changes since the Data Protection Directive

Unlike the Data Protection Directive, the GDPR has introduced fines. The Directive stated merely 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."[67] This, obviously, did not require the implementation of administrative fines. The Article 29 Working Party Guidelines

---

[66] *Id.* art. 83. The corresponding Recital 148 provides:

> 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 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.

Id. ¶ 148.

[67] *See* Data Protection Directive, *supra* note 17, art. 24.

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."[68] In line with GDPR recitals, especially Recital 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 their respective legal systems, which necessitated those two states to organise their rules differently.[69] As a result, Recital 151 provides that "in Denmark the fine is imposed by competent national courts as a criminal penalty."[70] It also provides that "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."[71]

In the Article 29 Data Protection Working Party Guidelines, on administrative fines, which are the focus of the next section, it is emphasised that the decision to fine someone will be appealable, presumably referring to future case law from national courts, and seemingly also the Court of Justice of the European Union.[72] 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.[73] In this context, any guidance that the DPAs may be able to procure is valuable. The

---

[68] Article 29 Data Protection Working Party Guidelines, *supra* note 34, at 8.

[69] *See* GDPR, *supra* note 1, ¶ 151 ("The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation.").

[70] *Id.*

[71] *Id.*

[72] Article 29 Data Protection Working Party Guidelines, *supra* note 34, at 8 ("Notably, the decisions in which the supervisory authorities exercise the fining powers conferred to them will be subject to appeal before national courts.").

[73] *See* GDPR, *supra* note 1, ¶ 10.

guidelines can, in spite of their non-binding character, be expected to become quite influential.

C. 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.[74] The Guidelines are "[i]ntended for use by the supervisory authorities to ensure better application" and effective enforcement of the GDPR,[75] and reflect a common understanding of the assessment criteria provided in Article 83(2) of the GDPR.[76]

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.[77] Administrative fines are not the only option, Article 58 of the GDPR offers a number of different measures.[78] The supervisory authority can issue warnings,[79] reprimands[80] or orders,[81] and withdraw certifications,[82] as well as impose fines.[83] All corrective measures should "adequately respond to the nature, gravity and consequences of the breach," and the "supervisory 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."[84] The objective of these measures can be "either to reestablish compliance with rules, or to punish unlawful behaviour (or both)."[85] The meaning of the broad terms "*effective, proportionate* and *dissuasive*" is to be determined by the supervisory authorities and the Court of Justice of the European

---

[74] *See* Article 29 Data Protection Working Party Guidelines, *supra* note 34, at 1.

[75] *Id.* at 4.

[76] *See* GDPR, *supra* note 1, art. 83(2).

[77] *See* Article 29 Data Protection Working Party Guidelines, *supra* note 34, at 9 ("The starting point is that the supervisory authority has to assess whether, considering the circumstances of the case at hand, the imposition of a fine is required.").

[78] *See* GDPR, *supra* note 1, art. 58(2).

[79] *See id.* art. 58(2)(a).

[80] *See id.* art. 58(2)(b).

[81] *See id.* art. 58(2)(c)-(e).

[82] *See id.* art. 58(2)(h).

[83] *See id.* art. 58(2)(i).

[84] Article 29 Data Protection Working Party Guidelines, *supra* note 34, at 6.

[85] *Id.*

Union in the years to come.[86] 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.[87]

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.[88] The second tier includes violations of individual rights protected by the GDPR, such as the basic principles for processing, the data subjects' rights to information, transfer rules, etc.[89] 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.[90] In both tiers, there are two assessments to be conducted: (1) whether a fine should be imposed, and (2) the amount of the fine.[91] In both assessments, supervisory authorities should consider all of the individual factors listed in Article 83(2).[92] However, the conclusions reached in the first step "may be used in the second part concerning the amount of the fine," avoiding the need to make the same assessment twice.[93] The Guidelines discuss how to interpret the various factors given in Article 83(2) above when making the two assessments.[94]

Even if it is first and foremost for the DPA to make the assessment in the individual case, the coherence mechanism remains available. The Guidelines further foresee that the EDPB

---

[86] *See id.* (emphasis added).

[87] *Id.* at 7.

[88] GDPR, *supra* note 1, art. 83(4).

[89] *Id.* art. 83(5).

[90] *See id.*; *see also* Article 29 Data Protection Working Party Guidelines, *supra* note 34, at 9 (discussing the assessment criteria in Article 83).

[91] Article 29 Data Protection Working Party Guidelines, *supra* note 34, at 9 (explaining that Article 83(2) "provides a list of criteria the supervisory authorities are expected to use in the assessment of both whether a fine should be imposed and of the amount of the fine").

[92] *See id.*

[93] *See id.*

[94] *See id.* at 9-16.

may make use of its competence in Article 65 to enact a decision within the dispute resolution:

> The EDPB, when competent according to [A]rticle 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 the 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[.][95]

The Guidelines also predict that the EDPB will give guidance on the application of Article 65 of the GDPR, providing more details on the type of decision to be made by the EDPB.[96]

IV. SANCTIONS AND REMEDIES UNDER THE GDPR—COMPOSITE OR NATIONAL?

A. Defining the Procedural Context for GDPR Sanctions and Remedies

Before the GDPR entered into force, "[t]he lack of harmonisation of national implementation laws with regard to the powers of DPAs" led to a high degree of diversity in regards to the regulation of sanctions.[97] 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.[98] With regard to damages, no equivalent actor, competent authority or similar, has been tasked with its

---

[95] *Id.* at 7.

[96] *Id.*

[97] Giurgiu & Larsen, *supra* note 36, at 344.

[98] *See* GDPR, *supra* note 1, art. 51(2) ("[T]he supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII."); *id.* art. 60(1) ("The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavor to reach consensus."); *id.* art. 63 ("In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.").

implementation. There is accordingly a manifest difference in approach between the two measures discussed here—damages and administrative fines. Where Article 83 of the 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.

B. GDPR Sanctions as part of a European Composite Administration

As 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.[99] The regulation of administrative fines is a central part of this governance structure, where 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 of the 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, courts might create administrative safeguards connected to handling matters, such as the duty to investigate diligently, the right of the parties involved to be heard, the obligation to reason decisions, and so forth. The Guidelines further acknowledge that national law "may set additional requirement on the enforcement procedure to be followed by supervisory authorities."[100] Such requirements may "include address notifications, form, deadlines for making representations, appeal, enforcement, [and] payment."[101] As mentioned above, Denmark and Estonia have organised their regimes for fining differently than the others due to national legal constraints.[102]

Member States are obliged to uphold the general principles of EU law and the Charter of Fundamental Rights of the European

---

[99] *See* HIJMANS, *supra* note 29, at 517; *see also supra* Part I(*B*).

[100] Article 29 Data Protection Working Party Guidelines, *supra* note 34, at 6.

[101] *Id.* (footnote omitted).

[102] *See* GDPR, *supra* note 1, ¶ 151; *see also supra* Part (I)(*B*).

Union when acting within the sphere of EU law.[103] According to case law, the obligation includes "the right to good administration," such as, for example, the abovementioned procedural safeguards of duty to investigate diligently, etc.[104] This does not necessarily exclude the application of national administrative procedural law since the EU general principles and the Charter often function as a minimum protection. As the Court of Justice of the European Union 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."[105] In areas that are comprehensively regulated by EU law, the Court of Justice of the European Union 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.[106] 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:

> 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.[107]

---

[103] *See supra* note 19.

[104] *See* Case C-604/12, H.N. v. Minister for Justice, Equal. and Law Reform, 2013 E.C.R. 00000, ¶ 36 ("[T]he Member states are required to ensure observance of fundamental rights and the general principles of Union law when they adopt decisions falling within the ambit of EU law. . . . There is therefore no doubt that Irish authorities must ensure respect for the right to good administration enjoyed by the persons concerned . . . ."); *see also* Case C-46/16, Valsts ieņēmumu dienests v. LS Customs Services, 2017 E.C.R. 00000, ¶ 39 ("As a preliminary point, it should be noted that the right to good administration, insofar as it reflect a general principle of EU law, has requirements that must be met by the Member States when they implement EU law." (internal citation omitted)).

[105] Case C-617/10, Åklagaren v. Åkerberg Fransson, 2013 E.C.R. 00000, ¶ 29.

[106] Case C-568/11, Agroferm A/S v. Ministeriet for Fødevarer, 2013 E.C.R. 00000, ¶¶ 49-51.

[107] *See* GDPR, *supra* note 1, ¶ 148.

In Article 58 of the GDPR, where DPAs' powers are listed, reference is made to EU and national law "in accordance with the Charter."[108] And lastly, in Article 83 of the GDPR, where the administrative fines are regulated, reference is made to EU law and national law as two independent sources.[109]

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. As a result, 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.

C. 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, and the main rule of national procedural autonomy can therefore be excepted to play a more decisive role 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.[110]

This Article raised the question of whether it is likely that the sophistication of the GDPR 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 Court of Justice of the European Union on the principle of equivalence, the answer to this question is presumably to be answered in the negative. The

---

[108] *Id.* art. 58(4) ("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.").

[109] *Id.* art. 83(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.").

[110] *See supra* Part I(*B*).

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 a "similar action" 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.[111] 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.[112] The latter, but not the former, provided a mechanism for revising a final decision. The Court of Justice of the European Union held that:

> 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 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.[113]

If remedies of an administrative nature are found to belong to a different branch of law than remedies of a civil law nature, then 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 would allow Member States to uphold stricter conditions and less beneficial procedural rules in relation to actions for damages for transgressions of the GDPR than

---

[111] *See* Case C-200/14, *Câmpean*, 2016 E.C.R. 00000, ¶¶ 55 ("[I]t must be pointed out that compliance with the principle of equivalence requires that actions based on an infringement of national law and similar actions based on an infringement of EU law be treated equally and not that there be equal treatment of national procedural rules applicable to proceedings falling within two different branches of law." (internal citation omitted)); *see id.* ¶ 56 ("The principle of equivalence must therefore be interpreted as precluding a Member State from providing procedural rules which are less favourable for applications for the repayment of a tax based on an infringement of EU law than those applicable to similar actions based on an infringement of domestic law.").

[112] *See* Case C-69/14, Dragoş Constantin Târşia v. Statul roman, 2015 E.C.R. 00000, ¶ 5 (explaining that the applicant "initiated civil proceedings").

[113] *Id.* ¶ 35.

for administrative sanctions for the same type of transgression. The question remains, though, as to 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.

V. IS THERE A POTENTIAL BRIDGE BETWEEN ARTICLE 82 AND ARTICLE 83 OF THE 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.[114] 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 remedies 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 Section IV(*A*) 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 Section IV(*B*), on the other hand, isolate the European influences from national laws 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

---

[114] *See* Adrienne de Moor-van Vugt, *Administrative Sanctions in EU Law*, *in* ADMINISTRATIVE SANCTIONS IN THE EUROPEAN UNION 607, 608 (Oswald Jansen ed., 2013).

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 coherence mechanisms of the 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" and "the number of data subjects affected and the level of damage suffered by them."[115] Existing here is an explicit connection between damages (supposedly non-material as well as material) and the rights and freedoms of natural persons. The corresponding section of the Article 29 Working Party Guidelines references the occurrence of damage suffered by data subjects.[116] The level of such damage is to be considered within the Article 83 assessment of which corrective measure to select.[117] 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.[118] Accordingly, it is clear that the compensatory principles of Article 82 have an impact on the imposition of administrative fines, according to the Article 29 Working Party Guidelines and Recital 148, if it does not already have an impact on deciding the amount, which is curious due to Article 83(2)'s inclusion of both steps of the assessment.[119]

Could the factors 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. On Article 83, the Guidelines simply say they provide no "explanations about the differences between administrative, civil or criminal law when imposing administrative sanctions in general."[120]

---

[115] *See* GDPR, *supra* note 1, art. 83(2)(a).

[116] Article 29 Data Protection Working Party Guidelines, *supra* note 34, at 11 ("If the data subjects have suffered **damage**, the level of the damage has to be taken into consideration.") (emphasis in original).

[117] *Id.*

[118] *See* GDPR, *supra* note 1, ¶ 148.

[119] *See id.* art. 83(2).

[120] *See* Article 29 Data Protection Working Party Guidelines, *supra* note 34, at 4.

As a tentative approach, a guiding principle could be that factors in Article 83(2) connected to the *data subject*, such as subsections (a)[121] and (g),[122] are highly relevant for Article 82. Further, factors connected to the *harmful act* itself and thus the controller or processor, including subsections (b)[123] and (c),[124] and possibly also (d),[125] (e)[126] and (f),[127] could be seen as relevant. Assessment criteria that are more closely connected to the *supervisory authorities* and the corrective measures of the GDPR: (h),[128] (i)[129] and (j)[130] are far from the compensatory purpose and the focus on the data subject, and should therefore not be taken into account under Article 82. They belong within the preventive aim of Article 83. The last criteria, subsection (k),[131] could of course 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

---

[121] GDPR, *supra* note 1, art. 83(2)(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").

[122] *Id.* art. 83(2)(g) ("the categories of personal data affected by the infringement").

[123] *Id.* art. 83(2)(b) ("the intentional or negligent character of the infringement").

[124] *Id.* art. 83(2)(c) ("any action taken by the controller or processor to mitigate the damage suffered by the data subjects").

[125] *Id.* art. 83(2)(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").

[126] *Id.* art. 83(2)(e) ("any relevant previous infringement by the controller or processor").

[127] *Id.* art. 83(2)(f) ("the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement").

[128] *Id.* art. 83(2)(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").

[129] *Id.* art. 83(2)(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").

[130] *Id.* art. 83(2)(j) ("adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42").

[131] *Id.* art. 83(2)(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").

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 of the GDPR, which may be quite high. From a broader perspective, this leads 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 damage—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 effective judicial remedies and due process are upheld within the composite structure? Only the future will tell.