Is Data Protection Law Growing Teeth?

The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR

by **Sebastian J. Golla**, Dr. iur, research assistant at Johannes Gutenberg-Universität Mainz*

Abstract: This article looks at the current lack of enforcement and sanctions in European Data Protection Law with a particular focus on administrative fines. It identifies reasons for the existing deficits in European Data Protection Law and analyses the potential of the new rules of the General Data Protection Regulation (GDPR) to compensate for those deficits. The article argues that the practical application of the new rules and the coordination of Data Protection Authorities (DPAs) in all member states of the EU are the key to more efficient sanctioning and enforcement through administrative fines.

Keywords: GDPR; European Data Protection Law; sanctions; administrative fines, enforcement; DPAs

Recommended citation: Sebastian J. Golla, Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR, 8 (2017) JIPITEC 70 para 1.

A. The Current Lack of Enforcement and Sanctions in Data Protection Law

1 It is common sense that the enforcement of Data Protection Law in Europe needs improvement.[1] A lack of effective sanctions has frequently been cited as one of the main reasons for existing enforcement deficits.[2] In general, effective sanctions are regarded as a prerequisite for achieving compliance with legal rules[3] and in theory, many different types of sanctions can be applied for violations of Data Protection Law, both under the existing national rules and the rules of the GDPR. In practice, however, the application of the sanctions is lagging behind the theoretical possibilities. Accordingly, Data Protection Laws are sometimes referred to as "toothless" or as "paper tigers".[4] From the perspective of legal philosophy, it can even be argued that a law without effective sanctions is not a law at all.

2 This article looks into the possible reasons for the lack of sanctions for violations of data protection rules, and focuses particularly on administrative fines. Specifically, the article examines the new rules of the GDPR concerning administrative fines

1 European Union Agency for Fundamental Rights, *Access to data protection remedies in EU member states* (Publications Office of the European Union, 2013), pp. 11 ff.; Thorben Burghardt and others, 'A Study on the Lack of Enforcement of Data Protection Acts' (Next Generation Society. Technological and Legal Issues - Third International Conference, e-Democracy 2009, Athens, Greece, September 2009); David Wright, 'Enforcing Privacy' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer 2016), pp. 13 ff.

2 Benedikt Buchner, *Informationelle Selbstbestimmung im Privatrecht* (Mohr Siebeck 2006), p. 299; Thomas Hoeren, 'Datenschutz als Wettbewerbsvorteil' in Erich Greipl (ed.), *100 Jahre Wettbewerbszentrale* (Deutscher Fachverlag 2012) p. 135, 136.

3 Thomas Raiser, *Grundlagen der Rechtssoziologie* (6th edn, Mohr Siebeck 2013), p. 253.

4 Jan Philipp Albrecht, 'Regaining Control and Sovereignty in the Digital Age' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer 2016), p. 473, 483; European Union Agency for Fundamental Rights, supra note 1, p. 47.

and attempts to forecast to what extent those rules may be able to compensate for the existing lack of enforcement and sanctions.

I. Administrative Fines and Other Sanctions

3 There are many different legal instruments to sanction violations of Data Protection Law. In a broad sense, a sanction can be defined as "the detriment, loss of reward, or coercive intervention annexed to a violation of a law as a means of enforcing the law".[5] In the context of Data Protection Law, this can include measures from the negative mentioning of a data controller in a supervisory authority's activity report ("naming and shaming") or an order by such an authority, as well as a civil-rights claim for damages by a data subject. Even though immaterial damages such as loss of reputation due to a mention in an activity report or a high-damage claim can be more painful for an enterprise in certain cases, technically administrative fines and criminal penalties are to be regarded as the most severe sanctions for data protection violations.

4 This article focuses on administrative fines for data protection violations. Administrative fines are of a higher practical relevance than criminal penalties.[6] While the Data Protection Directive 95/46/EC (DPD) does not specifically mention or require administrative fines for Data Protection violations,[7] most EU member states have implemented such sanctions in their Data Protection Acts.[8] However, there are big differences in the maximum amounts of administrative fines between the different member states.[9] While Romanian Law (maximum circa 11,000 €)[10] and Slovenian Law (12,510 €)[11] allow for relatively low fines, Spanish (600,000 €)[12] and UK Laws (500,000 £)[13] have much higher thresholds.

II. Deficits in the Application of Administrative Fines

5 In this section, I discuss the possible reasons behind the deficit of sanctions with a particular focus on the application of administrative fines.[14] Hereby I especially look at the role of the data subjects and the sanctioning authorities. For the sake of improved comprehensibility, this article operates under the assumption that DPAs have the competence to impose administrative sanctions for data protection violations, as is the case with most DPAs in Europe.[15]

1. Lack of Interest and Resources

6 If data subjects or authorities gain knowledge of a violation of Data Protection rules, it is their responsibility to initiate a procedure, which can eventually lead to an administrative fine. However, there are several reasons why the involved actors often do not make such an effort.

a.) The Role of Data Subjects

7 First, there are different conceivable reasons for data subjects to avoid initiating proceedings that could lead to administrative sanctions for data controllers. Among the very limited empirical material on the matter, a recent study conducted by the European Union Agency for Fundamental Rights gives some insight into the question.[16] The study looks at the factors that prevent subjects from seeking remedies or initiating procedures after they have experienced data protection violations.[17] Several

5 *Merriam-Webster's Collegiate Dictionary* (11th edn, 2004).

6 European Union Agency for Fundamental Rights, supra note 1, p. 21, Sebastian J. Golla, *Die Straf- und Bußgeldtatbestände der Datenschutzgesetze* (Duncker & Humblot 2015), pp. 199 ff.

7 Art. 24 DPD leaves the regulation of administrative fines at the discretion of the member states; cf. Paul De Hert and Gertjan Boulet, 'The Co-existence of Administrative and Criminal Law Approaches to Data Protection Wrongs' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer 2016), pp. 359 ff.

8 Paul De Hert and Gertjan Boulet, supra note 7, pp. 361 ff. give an overview of criminal penalties and administrative fines.

9 Cf. European Union Agency for Fundamental Rights, supra note 1, p. 21.

10 Maximal fine of 500 million Romanian leu under Art. 33 Law No. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data.

11 Article 91 Personal Data Protection Act.

12 Article 45 para. 3 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

13 The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 para. 2.

14 Cf. for a more detailed analysis Sebastian J. Golla, supra note 6, pp. 213 ff.

15 There are, of course, exceptions in certain states such as Kosovo (cf. Njomeza Zejnullahu, 'Imposition of Monetary Sanctions as a Mechanism for Protection of Personal Data: Comparative Analysis of Kosovo and Slovenia' (2016) 2 Eur. Data Prot. L. Rev. 80, 82), Austria (cf. Paul De Hert and Gertjan Boulet, supra note 7, p. 363) or the German State Baden-Württemberg.

16 European Union Agency for Fundamental Rights, supra note 1.

17 European Union Agency for Fundamental Rights, supra note 1, pp. 30 ff.

of these explanations apply to administrative fine proceedings in particular. The study distinguishes between "[I]ssues related directly to the procedure" such as the duration and the costs of the procedure, a "[l]ack of information or knowledge", and "[s]pecific personal and other reasons that made individuals uneasy about initiating the procedures."[18]

8 In a broader sense, the so-called "rational apathy"[19] or "rational disinterest" of data subjects affected by data protection violations can be identified as the main reason for choosing a path on inaction. From the perspective of the data subject, the effort to initiate a procedure can seem disproportionately large compared to the possible outcome. Violations of Data Protection Laws are often not regarded as important enough to take steps against them, especially if they do not affect financial interests and do not involve "sensitive" areas of life such as financial matters or the workplace.[20]

9 While there are several cases where data protection violations can have immediate effects on data subjects,[21] there seem to be even more scenarios where this is not the case and the impact of a data protection violation will only become perceptible a certain time after the initial violation has taken place. This is connected with the typical characteristic of Data Protection Law to protect individual rights in the forefront of further violations. As the German Constitutional Court has stated in its decisions on the basic right to informational self-determination, which is the basis of German Data Protection Law, "such an endangerment situation can already arise in the run-up to concrete threats to specific legal interests, in particular if personal information can be used and linked in a manner which the person concerned can neither detect nor prevent."[22]

10 Furthermore, the fear of potential unsavoury effects can reflect negatively on the individual's interest in filing complaints and initiating procedures. The potential unsavoury effect of an "emotional burden" can be a reason to avoid filing complaints.[23] Second, the fear of negative consequences inflicted by another party can also impede potential complainants.[24] This especially applies in cases where data subjects and violators are in a relationship of dependency.[25] The classic example for this is the situation where the data subject is the violator's employee fearing dismissal if a data protection violation is reported.

11 Individual apathy can especially become a problem in the case of data protection violations with a wide "scatter band", that is, in cases where the violation affects many persons but only has a negligible effect on each single individual.[26] While it may seem rational for each single individual to refrain from filing a complaint, the cumulative effect as such would require a sanction.

b.) The Role of Data Protection Authorities

12 While DPAs can help to compensate for the disinterest on the part of the data subjects, this is only possible to a certain extent. A big share of the work of DPAs is following up on complaints made by citizens. This means that if a data subject does not turn to an authority to initiate a procedure, the chances that a data protection violation is fined significantly decrease. The staffing capacities of authorities often do not allow them to conduct investigations out of their own initiative.

13 Other aspects that can stand in the way of imposing fines follow from the legal mandates of DPAs and their organisation. The main task of DPAs is to operate as a supervisory authority. At the same time, imposing fines for data protection violations is not a classical supervisory task. Supervisory activities are rather based on a cooperative and consulting approach. Those supervisory activities require a certain mutual trust between authorities and data controllers, which can hardly be established if there is a latent threat of imposing administrative fines.[27] Most data protection authorities do not strictly differentiate between their supervisory and sanctioning functions.[28] This leads to a conflict of objectives within the authorities.[29]

14 Several authorities have made it clear that their priority, rather than repressive action, is the

18 European Union Agency for Fundamental Rights, supra note 1, p. 30.

19 Kai von Lewinski 'Zwischen rationaler Apathie und rationaler Hysterie – Die Durchsetzung des Datenschutzes' (2013) 1 Privacy in Germany 12.

20 Cf. European Union Agency for Fundamental Rights, supra note 1, p. 30.

21 Cf. with several examples European Union Agency for Fundamental Rights, supra note 1, p. 28.

22 BVerfGE 120, 274, 312.

23 European Union Agency for Fundamental Rights, supra note 1, p. 30.

24 European Union Agency for Fundamental Rights, supra note 1, p. 32.

25 European Union Agency for Fundamental Rights, supra note 1, p. 30; Thilo Weichert, 'Datenschutzstrafrecht - ein zahnloser Tiger?' (1999) 19 NStZ, 490, 492.

26 Benedikt Buchner, supra note 2, p. 311.

27 Cf. Thilo Weichert, 'Regulierte Selbstregulierung – Plädoyer für eine etwas andere Datenschutzaufsicht' (2005) 21 Recht der Datenverarbeitung 1, 5.

28 One exception is the Bavarian Data Protection Authority which has made this distinction perfectly clear to the public, Bavarian Data Protection Authority, *Activity report 2010/2011*, p. 94.

29 See in more detail Sebastian J. Golla, supra note 6, pp. 216 ff.

prevention of future violations by cooperating with data controllers.[30] Consequently, the discretion of these authorities in imposing sanction is strongly influenced by the cooperative and consulting approach, which leads to a restrained practice.[31] In recent years, however, several authorities have begun to focus more on the enforcement of Data Protection Laws and have stated that they are making more use of their sanctioning competences.[32] This development has been reflected in the recent increase in fines for Data Protection violations in Europe.[33] One example for this changing practice is the UK. The Information Commissioner's Office (ICO) as the country's competent DPA, which has had the power to impose fines since April 2010, had only sparsely imposed administrative fines in the past.[34] However in October 2016, the recently appointed Information Commissioner Elizabeth Denham imposed a record fine of £400,000 against the telecommunications provider TalkTalk.[35] In her first speech as Information Commissioner, Denham said that "[t]he ICO will do its bit by focusing our advisory, education, investigatory and enforcement work on consumer control, transparency and fairness", but also pointed out the possibilities to impose high administrative fines under the GDPR and announced an intent to "use the stick in the cupboard when necessary."[36]

15 In contrast, a European example for a changing approach from strict administrative fines towards less rigid sanctions is the Spanish DPA Agencia Española de Protección de Datos (AEPD). While the AEPD is traditionally among the most active DPAs in Europe in terms of imposing administrative sanctions,[37] the number of cases and the amount of fines has been decreasing over the past years.[38] This is to some extent due to legal reforms,[39] but also because of the AEPD's exercise of discretion. In its latest report for the year 2015, the AEPD announced that it continued its tendency towards a decrease in administrative fines, planning to use other measures to correct data protection violations and to rather implement administrative sanctions as an ultima ratio.[40]

16 To avoid the described conflict of objectives and to enable the authorities to act both in a preventive and repressive manner, a clear separation between those two functions would be necessary. However, this separation proves to be difficult from a practical point of view. Authorities do not have the necessary budget or manpower to keep this tasks seperate and to focus more on imposing administrative fines.[41] Some smaller DPAs have a hard time making use of their very sanctioning competences in the first place.[42]

2. Lack of Information, Lack of Awareness and Legal Uncertainty

17 While a decision in favour of "rational apathy" requires knowledge and awareness that a data protection violation has occurred, in several cases even this requirement is lacking. Lack of information regarding existing rules and a corresponding lack of

30 For instance Hamburg Commissioner for Data Protection and Freedom of Information, *23. Tätigkeitsbericht Datenschutz 2010/2011*, p. 197; North Rhine-Westphalia Commissioner for Data Protection and Freedom of Information, *21. Datenschutz- und Informationsfreiheitsbericht 2011/2012*, p. 19; Independent Centre for Privacy Protection Schleswig-Holstein, *34. Tätigkeitsbericht 2013*, p. 24.

31 Matthias Lindhorst, *Sanktionsdefizite im Datenschutzrecht* (Peter Lang 2010) 42.

32 Alexander Dix, 'The International Working Group on Data Protection in Telecommunications: Contributions to Transnational Privacy Enforcement' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer 2016), p. 183; cf. Berlin Commissioner for Data Protection, *Jahresbericht 2009*, p. 85: "Due to the increasing number of uncovered massive data protection violations, we have given up the rather restrictive application of administrative fines as an ultima ratio in the last years."

33 Paul De Hert and Gertjan Boulet, supra note 7, pp. 364 f.

34 European Union Agency for Fundamental Rights, supra note 1, p. 21; Hazel Grant and Hannah Crowther, 'How Effective Are Fines in Enforcing Privacy?' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer 2016), pp. 287 f.

35 ICO, 'TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack' (*ICO*, 5 October 2016) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/> accessed 29 October 2016.

36 Elizabeth Denham, 'Transparency, trust and progressive data protection' (*ICO*, 29 September 2016) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/09/transparency-trust-and-progressive-data-protection/> accessed 29 October 2016.

37 Artemio Rallo Lombarte, 'The Spanish Experience of Enforcing Privacy Norms: Two Decades of Evolution from Sticks to Carrots' in David Wright and Paul De Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer 2016), p. 123 ff.; cf. also European Union Agency for Fundamental Rights, supra note 1, p. 21.

38 Agencia Española de Protección de Datos, *Memory 2015*, p. 36.

39 Artemio Rallo Lombarte, supra note 37, p. 123, 137 ff.

40 Agencia Española de Protección de Datos, supra note 38, p. 35 f.

41 Corinna Holländer, 'Datensündern auf der Spur, Bußgeldverfahren ungeliebtes Instrument der Datenschutzaufsichtsbehörden? ' (2009) 25 Recht der Datenverarbeitung 215, 222; Thilo Weichert, supra note 27 1, 6; cf. also European Union Agency for Fundamental Rights, supra note 1, p. 46.

42 For instance, the DPA of the German state Brandenburg only has one part-time employee to prosecute administrative offences; Commissioner of the State of Brandenburg for Data Protection and Access to Information, *16. Tätigkeitsbericht 2010/2011*, p. 158.

awareness in the data subjects are further reasons that can prevent administrative fine proceedings from being initiated. The recent study by the European Union Agency for Fundamental Rights has concluded that "[m]ost people do not know where to find information on the laws governing data protection violations and appropriate remedies, and are not aware of the organisations and institutions offering legal advice and support."[43]

18 Another issue that affects the application of administrative fines and other sanctions is the high degree of legal uncertainty in Data Protection Law. Many regulations operate with terms which leave a lot of room for interpretation. It is often hard to predict whether the processing of personal data is legal. Determining this often requires a balance of the affected interests in a single case.[44] This uncertainty has a negative impact on the possibility of effective compliance. Additionally, it can lead to a restrained use of sanctions. First, the data subjects will have a hard time determining whether a violation has occurred, which can prevent them from filing complaints. Second, working with uncertain rules makes it more difficult for DPAs to justify administrative fines. The concerns of some DPAs regarding the uncertainty of Data Protection Laws might even go so far that the rules of Data Protection Law are not applied due to the assumption that they might violate the constitutional rule of law.

B. Changes under the GDPR

19 The GDPR focuses on effective sanctions for data protection violations. Already in November 2010 the Commission announced in a Communication that it was seeking to "assess the need for strengthening the existing provisions on sanctions, for example by explicitly including criminal sanctions in case of serious data protection violations, in order to make them more effective."[45] Recitals 11 and 13 of the GDPR state that equivalent sanctions for data protection infringements are one essential requirement to ensure the "[e]ffective protection of personal data throughout the Union" and "a consistent level of protection for natural persons throughout the Union."

20 In this section, I briefly discuss the administrative fines newly introduced by the GDPR. Then I discuss to what extent the new rules of the GDPR may be able to address the current challenges.

I. The New Administrative Fines

21 The administrative fines under Article 83 GDPR are the strongest sanctioning instrument directly provided by the regulation. The fines that go up to 20,000,000 €, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, have received a lot of public attention. They have been interpreted as a legislative signal to US-American internet enterprises such as Alphabet or Facebook.[46] The fines in Article 83 GDPR are exceeding the fines in national laws both in the maximum amounts and in scope for offences entailing either negligent or intentional conduct. Even if this is not explicitly stated in Article 83 GDPR, it follows from the principle of culpability enshrined in Article 48 paragraph 1, Article 49 paragraph 3 Charter of Fundamental Rights of the European Union.

1. The Offences

22 Article 83 paragraphs 4 – 6 GDPR mainly cover data protection violations by controllers (Article 4 (7) GDPR) and processors (Article 4 (8) GDPR). The administrative offences refer to approximately 50 provisions of the GDPR.

23 Offences under Article 83 paragraph 4 GDPR are subject to administrative fines of up to 10,000,000 €, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year. Paragraph 4 (a) refers to the obligations of controllers and processors in Chapter 4 GDPR. Among many other provisions, the rule refers to Article 25 GDPR, which sets requirements for data protection by design and by default. Other offences, which could potentially become important in practice, include violations of the obligations to cooperate with supervisory authorities (Article 31 GDPR) and to appoint a data protection officer (Article 37 GDPR). Para 4 (b) and (c) include certification bodies (Article 43 GDPR) and monitoring bodies (Article 41 paragraph 1 GDPR) as special addressees for administrative fines.

24 Offences under Article 83 paragraph 5 and 6 GDPR are subject to administrative fines of up to 20,000,000 €, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year. Here, especially paragraph 5 (a) has a broad scope and high relevance. Under paragraph

43 European Union Agency for Fundamental Rights, supra note 1, p. 35.

44 Especially under Article 7 (f) DPD, cf. Sebastian J. Golla, supra note 6, pp. 163 ff.

45 Commission, 'A comprehensive approach on personal data protection in the European Union' COM(*2010*) *609 final*, p. 10.

46 Hazel Grant and Hannah Crowther, supra 34, p. 287, 291.

5 (a) infringements of the basic principles for processing personal data constitute administrative offences. This includes any unlawful processing against Article 6 GDPR. Under paragraph 5 (b) a violation of the rights of the data subject constitutes an administrative offence, paragraph 5 (c) refers to the rules on the transfers of personal data to third countries or international organisations in Chapter V GDPR. Under paragraph 5 (c), violations of member states' provisions, which have been adopted under the opening clauses in Chapter IX GDPR are subject to sanctions. Those provisions potentially include data processing for journalistic purposes and the purposes of academic, artistic or literary expression (Article 85 GDPR) or processing in the context of employment (Article 88 GDPR). Under paragraph 5 lit. (e) the non-compliance with orders of supervisory authorities and the failure to provide access to information are subject to fines. Next to this, the additional offence for the non-compliance with orders by the supervisory authority in paragraph 6 seems redundant.

2. General Conditions for Imposing Administrative Fines and Rules for Discretion

25 In case of a violation, the GDPR considers the imposition of an administrative fine as a rule according to Recital 148 sentence 1. That a fine is not necessary in each case follows from Recital 148 sentence 2, which states that only "[i]n 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." This novelty in the GDPR is important for the fining practice since it restrains the discretion that authorities might have for imposing sanctions under national laws.[47]

26 According to Article 83 paragraph 1 GDPR, fines "shall in each individual case be effective, proportionate and dissuasive". Those criteria are based on the European Court of Justice's jurisdiction regarding the regulation and imposition of sanctions by member states in the event of violations of Laws of the European Union.[48] To be effective and dissuasive, fines must have a certain preventive effect. However, those criteria leave a lot to the discretion of the competent authorities. The criterion of proportionality requires considering the circumstances of each individual case when imposing a fine.[49] The requirement of proportionality can also be applied in favour of data controllers, protecting them from inadequate fines. For instance, it has to be taken into account which fines have been imposed against competitors in the event of similar infringements.[50] This can be regarded as a specific regulation of the proportionality principle enshrined in Article 49 paragraph 3 Charter of Fundamental Rights of the European Union, which applies to penalties as well as to administrative fines.[51]

27 The requirement of proportionality is also reflected in the criteria in Article 83 paragraph 2 GDPR. The criteria of discretion regulated here concern both the question when an administrative procedure is to be initiated and the admeasurement of the administrative fine at the end of the procedure. The depth of detail with which the criteria of discretion have been regulated is unprecedented for a EU regulation. The criteria are inspired by the Commission's practice of administrative fines in Competition Law under Article 23 paragraph 2 lit. a) Council Regulation (EC) No 1/2003,[52] which is documented in guidelines.[53] According to Article 70 paragraph 1 (k) GDPR, the European Data Protection Board shall also draw up guidelines for supervisory authorities concerning the setting of administrative fines pursuant to Article 83 GDPR.

28 The criteria in paragraph 2 refer to the violation itself ((a), (b) and (g)), the precedent ((d), (e), (i) and (j)) and the subsequent behavior of the violator ((c), (f) and (h)). Beyond that, the general clause in paragraph 2 makes it possible to give regard to any other aggravating or mitigating factor applicable to the circumstances of the case. The principle of proportionality under paragraph 1 as well as the principle of certainty enshrined in Article 49 paragraph 1 Charter of Fundamental Rights of the European Union require a coherent and predictable imposition of administrative fines. In practice, this will require a union-wide cooperation of the competent authorities. According to Recital 150 sentence 5, the consistency mechanism (Article 63 ff. GDPR) may be used to promote a consistent application of administrative fines.

47 For instance, in German Law Section 47 para. 1 Act on Regulatory Offences gives a wider discretion to German authorities to prosecute administrative offences.

48 Case 68/88 *Greek Maize* [1989] ECR I-2965; Case 326/88 *Hansen* [1990] ECR I-2911.

49 Cf. Helmut Satzger, *Die Europäisierung des Strafrechts* (Carl Heymanns 2001) p. 372.

50 Gregor Thüsing and Johannes Traut, 'The Reform of European Data Protection Law: Harmonisation at Last?' (2013) 48 Intereconomics 271, 275.

51 Hans Jarass, *Charta der Grundrechte der Europäischen Union* (3rd edn, 2016), Article 49 para. 7.

52 Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty.

53 Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No 1/2003, paras. 27 ff.

3. Amount of Fines

29 The maximal amount of fines under Article 83 paragraph 4 to 6 has been a controversial subject in the legislative procedure. While Article 79 paragraph 2a (c) GDPR in the Parliament's version contained fines with a maximum amount of 100,000,000 € or of up to 5% of the total worldwide annual turnover of an undertaking, Article 79a GDPR in the Council's version only proposed a maximum of 250,000 € or up to 0.5% of the total worldwide annual turnover for certain violations.

30 Additionally, the calculation of the maximum amount poses some difficulties if it is based on the annual turnover. The practically relevant question is how the term "undertaking" in Article 83 is to be interpreted and if it covers corporate groups (like, for instance, Alphabet Inc.) or only single (subsidiary) companies.[54] The high economical relevance of this question becomes clear when looking at the large differences between turnovers of corporate groups and single companies.

31 According to Recital 150 sentence 3, "where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes." The term "undertaking" in Articles 101 and 102 TFEU is interpreted in a broad sense by the European Commission and the European Court of Justice. In the context of Competition Law the economic activity is decisive for the understanding of the term "undertaking".[55] In the words of the European Court of Justice, "the concept of an undertaking encompasses every entity engaged in an economic activity, regardless of the legal status of the entity and the way in which it is financed".[56] Therefore, "undertakings" in European Competition Law have been defined as "economic units which consist of a unitary organization of personal, tangible and intangible elements which pursues a specific economic aim on a long-term basis".[57] This can include entities consisting of multiple natural or legal persons.[58] In particular, a parent company and a subsidiary are to be considered an economic unit if the "subsidiary does not decide independently upon its own conduct on the market, but carries out, in all material respects, the instructions given to it by the parent company".[59]

32 However, one can also interpret the term "undertaking" similar to the term "enterprise" in Article 4 (18) GDPR. This would mean that only one natural or legal person could be regarded as an "undertaking", but not a group of companies. This interpretation is supported by the fact that several language versions of the GDPR use an identical term for what is described as an "undertaking" in Article 83 GDPR and as an "enterprise" Article 4 (18) GDPR (English version).[60]

33 Nonetheless, the interpretation following Recital 150 sentence 3 clearly corresponds with the legislator's will. The use of identical terms in Article 4 (18) GDPR and Article 83 GDPR in several language versions seems technically flawed and unfortunate. Recitals may specify the operative part of a regulation but may not establish incoherencies.[61] Here, the interpretation of Article 83 GDPR according to Recital 150 sentence 3 does not seem incoherent with Article 4 (18) GDPR. The rules of the GDPR are to "be interpreted and applied in the light of the versions existing in the other official languages"[62] to achieve a uniform interpretation. The different language versions show that the terms in Article 4 (18) GDPR and Article 83 GDPR are not necessarily identical, since several language versions use different terms in both provisions.[63]

34 As a result, "undertakings" under Article 83 GDPR can consist of several legal persons. Therefore, the total turnover of a corporate group will be decisive for the calculation of an administrative fine.[64]

54 Cf. Kai Cornelius, 'Die datenschutzrechtliche Einheit als Grundlage des bußgeldrechtlichen Unternehmensbegriff nach der EU-DSGVO' (2016) 5 Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht 421 ff.; Sebastian Faust, Jan Spittka and Tim Wybitul, 'Milliardenbußgelder nach der DS-GVO? Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz' (2016) 6 Zeitschrift für Datenschutz 120; Gerald Spindler, 'Die neue EU-Datenschutz-Grundverordnung' (2016) 69 Der Betrieb 937, 946 f.

55 Wolfgang Weiß, Art. 101 AEUV in Christian Calliess and Matthias Ruffert (eds), *EUV/AEUV* (C.H. Beck 2016), para. 25.

56 Case C-41/90 *Höfner and Elsner* [1991] ECR I-1979; cf. also Case C-205/03 P *FENIN* [2006] ECR I-6295.

57 Case T-11/89 *Shell* [1992] ECR II-757; cf. Wolfgang Weiß, supra note 55, para. 25.

58 Cf. Case 48/69 *Imperial Chemical Industries* [1972] ECR 619.

59 Case C-97/08 P *Akzo Nobel* [2009] ECR I-8237.

60 The German version for instance uses the term "Unternehmen" in both provisions. The French, Spanish and Italian version also use identical terms.

61 Case C-344/04 *International Air Transport Association* [2006] ECR I-403.

62 Case C-484/14 *McFadden* [2016].

63 Besides the English version, for instance the Bulgarian version uses different terms in Art. 83 ("предприятие") and Art. 4 (18) ("дружество") GDPR.

64 This opinion is shared by the Bavarian Data Protection Authority, 'Sanktionen nach der DS-GVO' (*BayLDA* 1 September 2016) <www.lda.bayern.de/media/baylda_ds-gvo_7_sanctions.pdf> accessed 29 November 2016.

II. Chances to Compensate Existing Deficits

35 The new rules of the GDPR and the ones on administrative fines in particular, have brought a lot of promises. For instance, Jan Philipp Albrecht, a Green Party MEP who was leading the negotiations between the Parliament and the Council on the adoption of the GDPR, has recently declared that with the application of the GDPR from 24 May 2018, "the lack of enforcement in the field of data protection provisions will end."[65] This section analyses to what extent the new legal rules have the potential to compensate the deficits described above.

1. Lack of Interest and Resources

36 The regulation of administrative fines in the GDPR does little to compensate for the lack of interest and resources of data subjects and DPAs in initiating procedures to fine data protection violations. Naturally, the potential of legal rules is limited in this regard. Looking at individual data subjects as potential complainants, it is difficult to create an environment that would encourage data subjects to initiate administrative fining procedures by legal rules since complainants do not economically profit from a successful procedure. However, complaints may slightly increase due to the more detailed rules on the DPA's discretion to impose fines in Article 83 paragraph 2 GDPR. A clearer and more predictable procedure might have positive effects on an individual's motivation to file complaints and to initiate procedures.

37 On the side of the DPAs, there are several issues which cannot be solved by the European regulation itself. In particular, the personal and financial resources of DPAs remain a problematic issue. One aspect that is tackled by the GDPR however is the conflict of objectives between the supervisory and fining functions of authorities described above. Again, the new rules about the discretion to impose sanctions in Article 83 paragraph 2 GDPR are a positive development to compensate for existing deficits. They are a first step towards a more effective union-wide cooperation between DPAs. They also might improve the sanctioning practices and mitigate the existing conflict of objectives. The fact that national data protection laws mostly do not offer specific guidance regarding administrative sanctions practices[66] entices DPAs to apply the standards of supervisory work to sanctioning work, which has led to a restrained practice so far.

38 Nonetheless, the GDPR does not distinguish clearly enough between the sanctioning and supervisory functions of the authorities. Article 58 paragraph 2 (i) and 83 paragraph 1 GDPR regard the imposition of administrative fines as one of several corrective powers of the DPAs as supervisory authorities. A stronger and clearer legal distinction between the functions as supervisory and sanctioning authorities would have been helpful to make this difference clearer.

2. Lack of Information, Lack of Awareness, and Legal Uncertainty

39 Regarding the issues of information, awareness, and legal certainty, the GDPR only partially helps to compensate for the deficits described above. Certainly, the GDPR and its legislative procedure have already raised the awareness for Data Protection Law and the potentially high fines. For instance, in a global survey report by the analyst firm Ovum in 2015, 52% of 366 IT decision makers said that they were expecting fines for their company under the GDPR.[67]

40 However, in terms of legal certainty, the GDPR is helpful only to a certain extent. On the one hand, the legal certainty will increase for enterprises that operate globally or in several European states since the substantial rules of Data Protection Law and the enforcement practices undergo a harmonisation. On the other hand, for smaller players, some DPAs, and also from the citizens' perspective, the new rules for administrative fines may become even harder to predict compared to the existing national laws. The reason for this is that the administrative offences under Article 83 paragraph 4 and 5 GDPR are extremely vague and unclear. Many of the almost 50 rules of the GDPR to which the offences refer do not draw a sufficiently clear line between legal and illegal behaviour.

41 For instance, Article 83 paragraph 4 a) in conjunction with Article 25 GDPR, which provides fines for infringements on the requirements for privacy by design and by default, does not seem compatible with the principle of certainty. From the criteria formulated in Article 25 paragraph 1 and 2 GDPR, the addressee of the rule will not be able to foresee if the measures they take fulfill the requirements of these rules.[68] The regulation does not provide a clear

65 Jan Philipp Albrecht, 'How the GDPR Will Change the World' (2016) 2 Eur. Data Prot. L. Rev. 287.

66 Paul De Hert and Gertjan Boulet, supra note 7, p. 364.

67 Ovum, *Data Privacy Laws: Cutting the Red Tape* (Report, 2015).

68 Malaika Nolde, 'Sanktionen nach der EU-Datenschutzgrundverordnung' in Jürgen Taeger (ed.), *Smart World – Smart Law?* (OIWIR 2016) 757, 768.

standard and does not answer the question regarding which technical and organisational measures are to be considered appropriate in an individual case to implement data-protection principles of the GDPR. In a similar manner, Article 83 paragraph 5 a) in conjunction with Article 6 paragraph 1 (f) GDPR fails to provide the addressee of the rules with sufficiently clear information on which conduct can be subject to a fine. According to Article 6 paragraph 1 (f) GDPR, the legality of processing personal data will depend on the result of a balance of interests in the individual case. Without further legal guidance, the outcome of this balance of interests will hardly be predictable in the majority of cases.

C. Conclusion: A Potential Game Changer but No Instant Cure

42 To conclude, the GDPR and its rules on administrative fines in Article 83 GDPR contain some positive steps to attenuate the existing lack of enforcement and sanctions in Data Protection Law. The GDPR's stronger focus on sanctions compared to the DPD, and especially the new fines, have gained some public attention. Both DPAs and companies in the IT-sector seem to be preparing for a stricter practice of fining. The existing conflict of goals in the DPAs is likely to be attenuated by the more specific rules for the discretion in imposing administrative sanctions. However, the GDPR still does not clearly distinguish between sanctioning and supervisory functions of DPAs. Regrettably, the GDPR also fails to compensate for some other legal problems which stand in the way of the effective sanctioning of Data Protection violations. In particular, the issue of legal uncertainty will cause headaches under the GDPR. Some central provisions to which Article 83 GDPR refers, such as Article 6 paragraph 1 (f) and Article 25 GDPR, do not live up to the principle of certainty and are not suitable for effective practical application.

43 The GDPR has the potential to become a game changer when it comes to sanctions and administrative fines in particular. However, the lack of enforcement will not immediately end with the application of the GDPR, as Jan Philipp Albrecht was quick to announce.[69] Certainly, the GDPR will lead to more frequent and higher fines for Data Protection violations in member states which have been operating on a low level so far.[70] But still, the question whether higher fines will be imposed on a regular basis in all member states remains open. It seems unlikely that eight-figure administrative fines will be imposed on a regular basis. The existence of a higher upper threshold does not necessarily mean that this threshold will ever be reached. In European Competition Law for example, the Commission has not yet exhausted the threshold for administrative fines, which are also calculated on the basis of the annual turnover.[71] All in all, it will require hard work and coordination of the European DPAs to significantly improve the overall situation of enforcement and sanctioning. Growing teeth can be a slow and painful process.

---

* This article is based on findings from the author's PhD thesis *Die Straf- und Bußgeldtatbestände der Datenschutzgesetze* [Criminal and Administrative Offences under Data Protection Acts] (Duncker & Humblot 2015). Since the thesis was submitted before the GDPR was passed and entered into force, the article especially focuses on the differences in the situation before and after the GDPR.

69 Jan Philipp Albrecht, supra 66. It is another question if an absolutely strict enforcement of data protection rules from one moment to another would even be desirable considering potential effects for the economy and freedoms of communication.

70 Hazel Grant and Hannah Crowther, supra 34, p. 287, 302.

71 Gregor Thüsing and Johannes Traut, supra note 50, 271, 276.