Putting a price on data protection infringement

Mona Naomi Lintvedt *

Key Points

- There is an assumption that the use of fines as an enforcement tool will have a deterrent effect and lead to compliance with the EU General Data Protection Regulation (GDPR). This article gives a critical analysis of the fines in Article 83 of the GDPR, and whether the introduction of elevated fines have led to the desired behavioural changes.
- The GDPR has no provisions that ensure harmonisation of the imposing and calculation of fines. This has already led to diverging practices by the Data Protection Authorities (DPAs). Neither does the GDPR require transparency about imposed fines. Without transparency, the deterrent effect of fines can be questioned.
- Monetary sanctions may not always lead to better compliance and ultimately better data protection for individuals. The GDPR has other enforcement measures that may have a more immediate effect in adjusting undesired processing of personal data, such as a temporary or definitive ban on processing which may be more harmful for a data-driven controller than a fine.
- The fines may function as punishment and deterrence, but not as restoration. Individuals who are affected by an infringement are not benefited by the imposed fine. Although Article 82 of the GDPR gives any person suffering material or non-material damage resulting from an infringement a right to compensation, the right is more theoretical than practical.
- The article concludes that adjustments should be made to ensure transparency and harmonisation. Also, changes should be considered to ensure that individuals are duly compensated in the event of damages suffered by data protection infringements.

Introduction

The EU General Data Protection Regulation (GDPR)[1] has a dual purpose: To protect individuals against infringement of their personal data and to ensure free flow of personal data in the internal market.[2] The regulation therefore has both a human rights and a business purpose.

The GDPR has substantial administrative fines for non-compliance with the regulation. The fines can be issued to the controller, ie the entity responsible for the processing of personal data,[3] and the processor, ie the entity processing personal data on behalf of the controller.[4] The fines are designed to make non-compliance a costly mistake for both large and small entities. The maximum fines are 10 or 20 million EUR depending on the seriousness of infringements. In the case of an undertaking, the maximum can be set to 2 or 4 per cent of the global annual turnover of the preceding financial year.[5]

The fines are imposed by the Data Protection Authority (DPA) in the respective EU Member States.[6] The use of fines as an enforcement tool may therefore

*Mona Naomi Lintvedt, Norwegian Research Centre for Computers and Law ('NRCCL'), Department of Private Law, University of Oslo, Norway. E-mail: m.n.lintvedt@jus.uio.no

Work on this article was carried out under the aegis of the research project 'Vulnerabilty in the Robot Society' ('VIROS'), funded by the Norwegian Research Council. Thanks are due to professor Jukka Mähönen and professor Lee A Bygrave for their encouragement and support, to colleagues at the NRCCL Beata Paragi and Dag Wiese Schartum, as well as to the anonymous reviewer for the very valuable suggestions and comments. The usual disclaimer applies.

Funding by the Norwegian Research Council, grant number 288285.

No conflict of interest.

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), OJ 2016 L 119/1.

2 GDPR, Art 1.

3 GDPR, Art 4(7).

4 GDPR, Art 4(8).

5 GDPR, Art 83.

6 With the exception of Denmark and Estonia, where the legal systems do not allow the DPAs to impose administrative fines. Instead, the fines are imposed as a criminal penalty and following a misdemeanour procedure respectively, cf GDPR, Art 83(9) and Recital 151. In Ireland, the administrative fines imposed by the DPA must be confirmed by the court, cf Data Protection Act 2018, ss 141–43.

diverge amongst the DPAs, dependent on their prioritizations and resources, and may also be influenced by national judicial practices on the use of financial sanctions. The GDPR has no instrument for the harmonisation of the use of fines as an enforcement tool except for voluntary cooperation between the DPAs.[7] The European Data Protection Board (EDPB), an independent legal body composed of one representative from each Member State DPA, shall contribute to consistent application of the regulation and cooperation between the DPAs.[8] The EDPB can issue guidelines for the setting of administrative fines, but has no authority to impose fines.[9] This differs from competition law, where the European Commission has the power to initiate enforcement procedures and imposing any remedy, including fines.[10]

Three years after the entry into force of the GDPR, the use of fines as an enforcement tool is still being cautiously tested by the DPAs. Whether the fines have led to better data protection for individuals is unclear. The general conditions for imposing administrative fines and the interpretation of Article 83 of the GDPR have been thoroughly covered by academia.[11] This article will not give an account of Article 83, but will discuss the effect of fines as a measure to ensure compliance from a law and economics perspective, and in particular whether the introduction of elevated fines have led to behavioural changes amongst the controllers.

Fines as a way to strengthen enforcement

The use of fines as sanctions for data protection infringement is not new to the data protection legislation. The previous Data Protection Directive[12] had a similar provision, but the amount of the fine was at the discretion of national law. The upper limit of fines ranged from 290 EUR in Lithuania to 601,000 EUR in Spain, while some Member States did not provide the DPA with the power to impose fines.[13]

The takeaway from the Directive was that fines are important incentives for compliance. The background for the sanctions in the GDPR were to propose 'fines that matter, which make you think twice . . . because the fines that exist . . . are minimal and you can ignore the Directive . . .; it doesn't matter'.[14] In order to strengthen the enforcement of the Regulation, penalties and administrative fines should be imposed for any infringement.[15] The administrative fines should be effective, proportionate and dissuasive,[16] a standard for sanctions which is present in several EU regulations and the case law of the European Court of Justice (CJEU).[17]

The large fines of the GDPR mirror the practice in competition law, and can be described as wealth-based punishment similar to US punitive damages.[18] By replicating the fines of competition law, the purpose of the administrative fines is to give an economic incentive to comply with the GDPR. Non-compliance will both punish the infringing entity and act as a market regulator.[19] The use of fines should be used 'either to re-establish compliance with the rules, or to punish unlawful behaviour (or both)'.[20]

The fines under competition law are aimed at punishment and deterrence. The purpose is to protect competition in a free-market economy. Infringement affects consumers by causing higher prices and lower quality.[21] The purpose of data protection regulation, on the other hand, is to protect people from abuse of their personal

7 GDPR, Art 51(2).

8 GDPR, Arts 68 and 70.

9 GDPR, Art 70(1)(k).

10 Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in arts 81 and 82 of the Treaty (OJ L 1, 4.1.2003, 1).

11 See *inter alia* Paul Voigt and Axel von dem Bussche, 'Enforcement and Fines under the GDPR' in P Voigt and A von dem Bussche (eds), *The EU General Data Protection Regulation (GDPR)* (Springer 2017) 201; Waltraut Kotschy, 'Article 83. General Conditions for Imposing Administrative Fines' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020) 1180; W Gregory Voss and Hugues Bouthinon-Dumas, 'EU General Data Protection Regulations Sanctions in Theory and in Practice' (2021) 37(1) Santa Clara High Technology Law Journal 1.

12 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, OJ 1995 L 281/31.

13 Commission Staff Working Paper. Impact Assessment. Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. SEC (2012) 72 final ('Impact Assessment'), 18 and Annex 2 para 10.10.2.

14 House of Commons Justice Committee. The Committee's opinion on the European Union Data Protection framework proposals. Third report of Sessions 2012–13. Volume 1. HC 572, para 87.

15 GDPR, Recital 148.

16 GDPR, Art 83(1).

17 Voss and Bouthinon-Dumas (n 11) 60.

18 Michael L Rustad and Thomas H Koenig, 'Towards a Global Data Privacy Standard' (2019) 71 Florida Law Review 365, 431.

19 Gregor Thüsing and Johannes Traut, 'The Reform of European Data Protection Law: Harmonisation at Last?' (2013) 48(5) Intereconomics 271, 275.

20 Art 29 Data Protection Working Party, 'Guidelines on the Application and Setting of administrative fines for the purposes of the Regulation 2016/679' (WP253, 13 October 2017), 6.

21 European Parliament, 'Fact Sheets on the European Union 2021. Competition Policy' <www.europarl.europa.eu/factsheets/en/sheet/82/competition-policy>. Please note that all following URLs referenced in

data and infringement of their privacy. Infringement of the GDPR does not necessarily have a direct economic consequence for individuals, although processing of personal data may be economically beneficial for businesses.

Except for stating that the Regulation would be strengthened with fines, there has been no further analysis of its behavioural effects. The drafting of the GDPR took a turn with the Snowden revelations in 2013, which further emphasized the need to use economic sanctions to punish misbehaviour.[22] The upper limit of the fines was increased from the original proposal, and there was an expectation that the GDPR and the accompanying sanctions would be directed at the large US tech companies in defence of European citizens and privacy values. Due to the extraterritorial scope of the GDPR, these companies would also be subject to the GDPR.

Economic theory on optimal deterrence teaches that the expected fine should equal the harm caused by the infringement, or alternatively the gain to the violator plus a certain safety margin. Depending on the probability of detection and punishment, the actual fine should be a multiple of this amount.[23] Thus, fines should be framed retributively and exacted publicly to have an effective deterrent effect.[24]

The largest fine for data protection infringement thus far was not issued under the GDPR, but under US privacy law. Facebook was fined a whopping 5 billion USD in 2019, 20 times higher than the next highest fine.[25] For the company, the fine equalled a month's revenue. In addition, Facebook was required to make changes in their services and introduce a privacy compliance programme. Although the fine may seem high, critics claimed it was set too low and would not lead to substantial changes in Facebook's practice. This was confirmed by the positive response from the market, with Facebook's stock price jumping by more than 1 per cent immediately after the case was settled.[26]

There is an assumption that the use of fines similar to what we find in EU competition law will have the appropriate punitive and deterrent effect. However, practice from competition law questions the effect of fines on behaviour. For example, Google has so far paid more than 9 billion USD in fines for violation of European competition rules, but the penalties have not resulted in any long-term changes in Google's behaviour; the company is as dominant as ever in the European market.[27] In a current anti-trust case filed against Google by the state of Texas, a fine of 160 billion USD, equivalent to the annual revenue of Google's online advertising operations, has been mentioned as necessary leverage to force the firm to change behaviour.[28]

A report from the European Court of Auditors evaluating the European Commission's merger control and antitrust proceedings, found that there has been no overall evaluation of the deterrent effect of fines in competition law, although the regulations have been in place for over a decade. The auditors recommend that the Commission take action to perform a study of the deterrent effect of fines, and update its fine-setting methodology in accordance with the findings.[29] Thus, replicating fines from competition law also replicates ignorance of the effect of fines.

Behavioural effects of anticipated fines

The potential magnitude of the GDPR fines has attracted much attention, and is often mentioned whenever the GDPR is mentioned. There are some indications that the prospect of fines has changed behaviour. Some of the behaviour may be due to the increased awareness of data protection, but considering that the EU has had similar legislation since 1998, it can be assumed that much of the change is in the emphasis on the fines.

The economic impact assessment of the GDPR estimated compliance costs to be a meagre 210 million EUR per annum in total for all entities that would be subject to the GDPR. The assumption was that there would be a strong reduction of compliance costs compared to the former Directive, and that 2.2 billion EUR

this paper were last accessed 11 November 2021, unless otherwise specified.

22 Moritz Laurer and Timo Seidl, 'Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation' *Policy and Internet* (25 June 2020) <doi.org/10.1002/poi3.246>.

23 Wouter P J Wils, 'E.C. Competition Fines: To Deter or Not to Deter' (1995) 15(1) Yearbook of European Law 17.

24 Tim Kurz, William E Thomas and Miguel A Fonseca, 'A Fine Is a More Effective Financial Deterrent when Framed Retributively and Extracted Publicly' (2014) 54 Journal of Experimental Social Psychology 170, 170–72.

25 Federal Trade Commission, 'FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook' (24 July 2019) <www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.

26 Julia Carrie Wong, 'Facebook to Be Fined $5bn for Cambridge Analytica Privacy Violations – Reports' *The Guardian* (San Francisco, 12 July 2019) <www.theguardian.com/technology/2019/jul/12/facebook-fine-ftc-privacy-violations>.

27 Simon Van Dorpe and Leah Nylen, 'Europe Failed to Tame Google. Can the U.S. Do Any Better?' *Politico* (21 October 2020) <www.politico.com/news/2020/10/21/google-europe-us-antitrust-431036>.

28 Leah Nylen and Renuka Rayasam, 'Google Could Face Trillions in Fines in Texas Antitrust Suit' *Politico* (23 December 2020) <www.politico.com/news/2020/12/23/google-texas-antitrust-suit-450188>.

29 European Court of Auditors, 'The Commission's EU Merger Control and Antitrust Proceedings: A Need to Scale up Market Oversight' Special report 24/2020.

in administrative burden would be 'virtually eliminated by the increased harmonisation'. It was admitted that there would be some additional compliance costs, but that a strong data protection regime in Europe would be a competitive advantage for the European economy.[30]

In reality, the introduction of the GDPR has led to massive implementation and compliance work for both private and public entities. The average implementation cost of Fortune 500 companies was estimated to be 16 million USD.[31] Other studies suggest that the value of the GDPR compliance market is 384.9 billion USD.[32] A noticeable way that the regulation has influenced behaviour is the creation of an extended market for GDPR consultancy, as well as an emerging insurance market.[33]

The fear of non-compliance has also led to other behaviour. Some companies, such as a British pub chain, chose to delete its customer e-mail database instead of having to deal with the risk of non-compliance.[34] Other companies are moving out of the EU and are not offering their services to European customers. This includes several websites that are no longer open to visitors from European IP addresses.[35]

Other companies have tried to avoid the jurisdiction of the GDPR rather than changing their practice. Facebook moved their UK users from the Irish subsidiary to California in 2021, following a similar move of all non-EU users in 2018.[36] With the possibility of the UK diverging from EU data protection legislation after Brexit, Facebook has taken the opportunity to move users from the EU to avoid the jurisdiction of the GDPR and decrease their liability.[37] Google has previously announced a similar move of their UK users.[38]

Effects of fines in the public sector

Article 83(7) of the GDPR leaves to the Member States whether administrative fines should be imposed on public authorities.[39] The initial proposal of the Irish Data Protection Act exempted public authorities from administrative fines, except for public authorities acting as undertakings. The reasoning was that although fines could have a deterrent effect, it would also reduce available funds for the provision of services to the public, which could lead to demands for replacement funding, which in turn 'could result in a wasteful, circular flow of funding'.[40] However, there were concerns that an exemption for public authorities could signal lower expectations for compliance; thus, the deterrent effect of fines would be vital to ensure a high level of data protection by public authorities.[41] Pressure during the consultation and drafting processes led to a two-fold scheme for public authorities: A public authority acting as an undertaking will be subject to the same administrative fine procedure as other undertakings, to avoid competition distortion when public and private bodies operate in the same market.[42] For public authorities not being undertakings, the maximum fine is set at 1 million EUR.[43]

In Belgium, public authorities are exempted from administrative fines, with the exception of those offering

30 Impact Assessment (n 13) 77.

31 Oliver Smith, 'The GDPR Racket: Who's Making Money From This $9bn Business Shakedown' *Forbes* (2 May 2018) <www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/>.

32 Fazal, 'The Cost of GDPR Compliance' *Medium* (31 January 2020) <https://medium.com/@drfazal/the-cost-of-gdpr-compliance-8e58a2b5232e>.

33 Darcy WE Allen and others, 'Some Economic Consequences of the GDPR' (2018) 39(2) Economics Bulletin 785.

34 Rowland Manthorpe, 'Wetherspoon Just Deleted Its Entire Customer Email Database – On Purpose' *Wired* (3 July 2017) <www.wired.co.uk/article/wetherspoons-email-database-gdpr>.

35 List compiled by VerifiedJoseph, updated 25 March 2019 <https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr>.

36 David Ingram, 'Exclusive: Facebook to Put 1.5 billion Users Out of Reach of New EU Privacy Law' *Reuters* (San Francisco, 19 April 2018) <www.reuters.com/article/us-facebook-privacy-eu-exclusive/exclusive-facebook-to-put-1-5-billion-users-out-of-reach-of-new-eu-privacy-law-idUSKBN1HQ00P>.

37 Natasha Lomas, 'Facebook to Move UK Users Out of EU's Privacy Jurisdiction Next Year, Post-Brexit' *Techcrunch* (16 December 2020) <https://techcrunch.com/2020/12/16/facebook-to-move-uk-users-out-of-eus-privacy-jurisdiction-next-year-post-brexit/>.

38 Madhumita Murgia, 'Google Moves UK User Data to US to Avert Brexit Risks' *Financial Times* (20 February 2020) <www.ft.com/content/135e5b66-53fb-11ea-90ad-25e377c0ee1f>.

39 According to an overview by the law firm White & Case, the Netherlands and Norway have no exemptions for public authorities. Austria, Belgium, Croatia, Finland, Germany, and Liechtenstein exempt public authorities from fines, while the majority of Member States have set fine caps ranging from 280 EUR to 10 million EUR for public authorities. Detlev Gabel and Tim Hickman, 'GDPR Guide to National Implementation: Q17 Administrative Fines, Penalties and Sanctions' (13 November 2019) <www.whitecase.com/publications/article/gdpr-guide-national-implementation#q17>.

40 Data Protection Bill 2018: Second stage. Seanad Éireann debate (8 February 2018) Vol 255 No 14 <www.oireachtas.ie/en/debates/debate/seanad/2018-02-08/9/>.

41 ibid. See also Elaine Edwards, '"Serious Concern" Over Exemption of Public Bodies from Data Protection Fines' *The Irish Times* (15 June 2017) <www.irishtimes.com/news/politics/serious-concern-over-exemption-of-public-bodies-from-data-protection-fines-1.3120643>; Elaine Edwards, 'Public Bodies Not Subject to Fines Under New Data Protection Bill' *The Irish Times* (1 February 2018) <www.irishtimes.com/news/crime-and-law/public-bodies-not-subject-to-fines-under-new-data-protection-bill-1.3377063>.

42 Head 23 of the General Scheme of Data Protection Bill (2017); Data Protection Act 2018 Explanatory Memorandum 19-20.

43 Data Protection Act 2018, s 141(4).

products and services in a market.[44] The exemption was contested as being discriminatory and in violation of the Constitution, but the Constitutional Court rejected the claim. The court pointed to the motivation in the preparatory works that the imposing of fines on public authorities would lead to a financial burden that could undermine the continuity of public services and jeopardize the exercise of a mission of public interest. The court stated that the use of fines is not the only enforcement measure to ensure compliance with the GDPR, and that the use of other corrective measures and penalties can be sufficiently dissuasive. Furthermore, the court underlined that the exemption from administrative fines would not affect the data subjects' right to compensation for damages.[45]

On the other hand, the Norwegian Personal Data Act, § 26 applies Article 83 of the GDPR to public authorities in full.[46] In public consultation on the legislation, the rationale was that the former data protection act had a similar provision. The argument was that there should be no difference in enforcement between public authorities and private entities. Some parties pointed out that a cap should be set on the fines or no fines given, since a fine would impact the budget and thereby the capability to finance public services. It was argued that the reputational damage would be a deterrent in itself.[47]

Since the GDPR entered into force, the Norwegian DPA has imposed several fines on public authorities. The symbolic and deterrent effects have been highlighted by the DPA in the decisions.[48] From an economic point of view, it can be questioned whether fines against public authorities will have a real effect (apart from appearances), since money is simply being moved from one public budget to another. Other enforcement methods may be more appropriate to ensure compliance and punish non-infringement in public sector entities.[49] One of the largest fines of 307,000 EUR was imposed on a municipality for an infringement that affected schoolchildren and their parents.[50] In principle, the inhabitants paid for the infringement three times. First, their privacy was compromised. Second, the fine will in effect be paid over the municipal budget, which in turn is financed through taxes and fiscal transfers from the state. Third, the use of budgetary funds can decrease the financing of public services. For the municipality, the resulting lack of public trust, embarrassment, and political consequences may be graver than the economic consequences of a fine.[51]

Lack of harmonisation

Disharmony in imposed fines

There are diverging practices across the Member States so far, both on the number of imposed fines and the amounts. The total number of fines imposed by the DPAs from May 2018 to May 2021 is 2208. However, half of the decisions are by the DPAs in Germany (606), Spain (279), and Italy (228), while a quarter of the fines are imposed by the DPAs in Bulgaria (172), Hungary (170), Slovakia (124), and the Czech Republic (106). For the remaining DPAs, the average number of fine decisions is 25, with seven DPAs[52] having imposed less than 10 fines each during this period.[53]

There was anticipation that the fines would be particularly suited to target large, mostly US-based, tech companies and force these companies to adopt more privacy-friendly policies. But few fines have been issued against tech companies thus far. Most of the global tech companies have their European headquarters in Ireland or Luxembourg due to their favourable tax regimes. Thus, the enforcement of the GDPR is under the jurisdiction of the Irish and the Luxembourg DPAs. Several complaints have been filed against these companies. Per

44 La loi du 30 Juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, art 221, §2.

45 La Cour constitutionnelle, Arrêt n° 3/2021 du 14 janvier 2021.

46 Lov om behandling av personopplysninger (personopplysningsloven) 15. juni 2018 nr. 38 [The Personal Data Act].

47 Prop. 56 LS (2017–2018) Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen, chapter 20.3.

48 See eg the final decision of a fine of 400,000 NOK (40,400 EUR) on Norwegian Customs, where the Norwegian DPA states that the fine is a clear signal with the aim of general assurance that public authorities will meet the expected level of compliance. Datatilsynet, 'Delvis omgjøring av vedtak om overtredelsesgebyr – Tolldirektoratet' (1 September 2019) 17 <www.datatilsynet.no/contentassets/bf78561e4fc948c0a417658f1cf76cca/tolldirektoratet-vedtak.pdf>.

49 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 Technical Approaches* (Springer 2016) <doi.org/10.1007/978-3-319-25047-2_13>.

50 The imposed fine was 3 million NOK, and was not appealed by the municipality. Datatilsynet, 'Vedtak om overtredelsesgebyr Bergen kommune. Melding om avvik i Vigilo 20/02181' (3 September 2020) <www.datatilsynet.no/contentassets/fd5c454b4eae4924af94943ba68002bf/20_02181-3-vedtak-om-overtredelsesgebyr--bergen-kommune.pdf>.

51 A hearing about the case was held by the City Council, and the Commissioner for Education and Sports withdrew from her position to avoid a no-confidence motion against the City Government. See Bergen kommune, 'Høring om Vigilo-saken' (14 January 2020) <www.bergen.kommune.no/politikk/bystyret/bystyreutvalgene/siste-nytt/horing-om-vigilo-saken>; 'Engø går av som byråd' (27 January 2021) <www.bergen.kommune.no/hvaskjer/barnehage-og-skole/engo-gar-av-som-byrad>.

52 Croatia, Finland, Iceland, Ireland, Liechtenstein, Luxembourg, and Slovenia.

53 All numbers are from European Data Protection Board, 'Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities' (5 August 2021) 16 <https://edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf>.

October 2021, the Luxembourg DPA has imposed one fine and the Irish DPA has imposed two fines against Big Tech.

The Luxembourg DPA imposed a fine of 746 million EUR against Amazon in July 2021. The DPA did not share any details about the case, citing professional secrecy, but confirmed that a decision was made[54] following the disclosure by Amazon in their quarterly earnings report.[55] It is by far the largest fine so far, but is not final since it is appealed by Amazon who will 'defend ourselves vigorously in this matter'.[56]

In December 2020 the Irish DPA concluded a much-anticipated case against Twitter. The infringement was minor, but the investigation took two years and preparation of a 200-page report before a conclusion was reached. The case was submitted to the consistency mechanism of Article 63 of the GDPR after other DPAs disputed the draft decision. The EDPB adopted a binding decision in accordance with Article 65(1)(a) of the GDPR, requiring the Irish DPA to increase the amount of the fine from the suggested 0.01 per cent of turnover.[57] The final decision imposed a fine of 450,000 EUR, equivalent to 0.018 per cent of the annual turnover.[58] In September 2021, the Irish DPA announced a fine against WhatsApp of 225 million EUR,[59] following a binding decision by the EDPB to increase the fine from the suggested 30–50 million EUR.[60] The fine is not final since it has been appealed by WhatsApp to the High Court, claiming it is disproportionate and infringing with its property rights.[61]

Impatience with the Irish DPA has previously led the French DPA to issue fines against Google, arguing that although Google is established in Ireland, the company's infringement would fall under French jurisdiction for services directed at French users since the Irish establishment had no decision-making powers over the processing in question. The French court agreed with this interpretation.[62]

Disharmony in calculating fines

The EDPB has adopted a guideline on administrative fines concerning criteria for the use of fines as sanctions.[63] There is no further guidance for the calculation of fines similar to the guidelines in competition law.[64] Although the DPAs are encouraged to cooperate,[65] there are no formal requirements for harmonisation of fines across the Member States, except in cross-border cases. The consistency mechanism of Article 63 of the GDPR has so far only been used twice in cases concerning administrative fines.[66]

The calculation and imposition of fines are thus left to the discretion of each DPA. As stated by the Irish DPA:

> In the absence of specific EU-level guidelines on the calculation of fines [. . .], I am not bound to apply any particular methodology. In practical terms, this means that I am not bound to use a base figure or fixed financial starting point for the assessment of the proposed fine.[67]

54 Commission nationale pour la protection de données, 'Décision concernant Amazon Europe Core S.à r.l.' <cnpd.public.lu/fr/actualites/international/2021/08/decision-amazon-2.html>.

55 US Securities and Exchange Commission, 'Amazon.com, Inc. Form 10-Q. For the Quarterly Period Ended June 30, 2021' <www.sec.gov/ix?doc=/Archives/edgar/data/0001018724/000101872421000020/amzn-20210630.htm>.

56 Ibid 13. According to media coverage, a spokesperson for the Tribunal Administratif has confirmed that Amazon filed an appeal in October 2021, 'Amazon fait appel de sa condamnation par la CNPD', *Luxemburger Wort* (15 October 2021) <www.wort.lu/fr/economie/amazon-fait-appel-de-sa-condamnation-par-la-cnpd-61698cb4de135b923668e6a2>.

57 European Data Protection Board, 'Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR' (9 November 2020) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_bindingdecision01_2020_en.pdf>.

58 Data Protection Commissioner Ireland, 'In the matter of Twitter International Company. Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018. DPC Case Reference: IN-19-1-1' (9 December 2020) 181 <https://edpb.europa.eu/sites/edpb/files/decisions/final_decision_-_in-19-1-1_9.12.2020.pdf>. The decision was confirmed by the court in October 2021, Data Protection Commissioner, 'Confirmation of Fine – Twitter International Company' (18 October 2021) <www.dataprotection.ie/en/news-media/press-releases/confirmation-fine-twitter-international-company>.

59 Data Protection Commissioner Ireland, 'In the matter of WhatsApp Ireland Limited. Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation. DPC Inquiry Reference: IN-18-12-2' (20 August 2021) <https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf>. WhatsApp, Inc. (as the parent company of WhatsApp Ireland Limited) and Facebook, Inc. were considered to constitute a single economic unit, and thereby a single undertaking with an estimated turnover of 85,965 billion USD, see p 248–57.

60 European Data Protection Board (n 57).

61 Charlie Taylor and Aodhan O'Faolain, 'WhatsApp Challenges DPC's €225 Million Fine' *The Irish Times* (16 September 2021) <www.irishtimes.com/business/technology/whatsapp-challenges-dpc-s-225-million-fine-1.4675957>. WhatsApp has also filed a case with the CJEU to challenge the Article 65 decision by the EDPB, Case T-709/21: WhatsApp Ireland v Comité européen de la protection des données.

62 Le Conseil d'État. 'Sanction infligée à Google par la CNIL' No 430810. <www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-19-juin-2020-sanction-infligee-a-google-par-la-cnil>.

63 WP29 (n 20).

64 Guidelines on the method of setting fines imposed pursuant to art 23(2)(a) of Regulation No 1/2003 (OJ C 210, 1.9.2006, pp 2–5).

65 GDPR, Art 51(2).

66 As of November 2021. See European Data Protection Board, 'Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism' <https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en> accessed 17 November 2021.

67 Data Protection Commissioner Ireland (n 58) 175–76.

The GDPR distinguishes the fine levels as fixed sums and a percentage of annual turnover, the latter being used in the case of undertakings. The term 'undertaking' is not defined in the GDPR, but refers to Articles 101 and 102 of the TFEU.[68] Neither article defines the term, and the reference must be understood as a reference to the case law concerning the definition of an undertaking under the TFEU.[69] The definition given by the CJEU in competition law is 'every entity engaged in an economic activity, regardless of the legal status of the entity and the way in which it is financed'.[70] The EDPB understands this to be an 'economic unit, which engages in commercial/economic activities, regardless of the legal person involved'.[71] This will require the DPAs to take into consideration the jurisprudence of competition law when assessing whether a controller is an undertaking and the extent of a group of undertakings, in the case of an economic unit consisting of several entities. There is already diverging practice on this point, as some DPAs do a thorough assessment of identifying the relevant undertaking, while others conclude without further investigation.[72]

The annual turnover is relevant to set the cap for the fine in the case of undertakings. Although turnover can indicate the level of deterrence necessary for a fine, it's not one of the factors to be considered in Article 83(2) of the GDPR when deciding on the amount of the fine. However, turnover seems to be used by DPAs not only to set the cap but also to determine the level of the fine. In a binding decision, the EDPB states that although Article 83(2) nor Article 83(3) of the GDPR refer to turnover, this should not be interpreted as being an exhaustive list and that it does not exclude turnover from being considered. In the view of the EDPB, turnover is relevant to setting a fine level that is effective, proportionate, and dissuasive. Furthermore, the EDPB points out that the similarities between the fine systems of competition law and the GDPR are such that the case law of the CJEU in competition law may serve to clarify questions on the imposing of fines in the GDPR. The EDPB argues that since consideration of turnover in the calculation of fines is an accepted practice in competition law, this can also be applied for Article 83 of the GDPR concluding that 'the turnover of an undertaking is not exclusively relevant for the determination of the maximum fine amount . . . , but it may also be considered for the calculation of the fine itself'.[73] The interpretation of the EDPB assumes that there must be an undertaking for the turnover to be relevant and further underlines the necessity of proper assessments of the relevant undertaking and turnover when imposing fines.

The German, Danish and Dutch DPAs have made standard models for calculation of fines. The DPAs have committed that they will no longer use the models if the EDPB agrees on a standard model. The German model is to categorize companies by their size and turnover and then calculate a basic value which is multiplied by a factor that depends on the severity of the offense.[74] The result is that the fine will increase with the turnover, rather than the severity of the infringement. The method can lead to large fines being issued for less severe infringements if the perpetrator is a large company. The Danish model defines standardised fines according to the size of companies based on their turnover, with adjustments based on the specific circumstances.[75] The Dutch model, on the other hand, sets standard fine brackets for different categories of infringements without reference to turnover. Similar infringements will therefore lead to similar fines, regardless of the turnover of the entity in question.[76]

Not only is there diversity in how the fines are calculated, but the DPAs have also varying methods of calculating turnover, as the GDPR does not define it. With

68 GDPR, Recital 150.

69 Kotschy (n 11) 1187–88.

70 See Lee A Bygrave and Luca Tosoni, 'Article 4(18). Enterprise' in Kuner and others (n 11) 248–51; Luca Tosoni, 'Article 4(19). Group of undertakings' in ibid 254–56.

71 WP29 (n 20) 6.

72 eg in the Twitter case, the Irish DPA discusses the relation between Twitter International Company and Twitter Inc to identify the relevant undertaking, with references to the TFEU and the practice of the CJEU. See Data Protection Commissioner Ireland (n 58) 176–79. By comparison, the Norwegian DPA in a draft decision imposing a fine of 25 million NOK to Disqus Inc., refers to a parent company, but without discussing whether there is a group of undertakings. See Datatilsynet, 'Advance notification of an administrative fine – Disqus Inc.' (2 May 2021) <www.datatilsynet.no/contentassets/8311c84c085b424d8d5c55dd4c9e2a4a/advance-notification-of-an-administrative-fine–disqus-inc.pdf>.

73 European Data Protection Board, 'Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR' (28 July 2021) 82–83. <https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf>.

74 Datenschutzkonferenz, 'Concept of the independent data protection authorities of the Federation and the Länder for the measurement of fines in proceedings against undertakings' (14 October 2019) <www.datenschutzkonferenz-online.de/media/dskb/20191126_dsk_fining_concept_en.pdf>.

75 Datatilsynet, 'Bødevejledning. Udmåling av bøder til virksomheder' (January 2021) <www.datatilsynet.dk/Media/1/9/B%C3%B8devejledning.pdf>.

76 Autoriteit Persoonsgegevens, 'Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2019)' (14 March 2019) <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-14586_0.pdf>.

the lack of common guidelines, each DPA seems to make their own interpretation of how turnover should be calculated. The Danish guidelines[77] refer to the definition of net turnover in the Accounting Directive, Article 2 nr 1(5) – 'the amounts derived from the sale of products and the provision of services after deducting sales rebates and value added tax and other taxes directly linked to turnover'.[78]

In their case against Twitter, the Irish DPA referred to the revenue stated by the firm in the annual report for the preceding year.[79] The Norwegian DPA, in a preliminary case against Grindr, relied on online articles about the firm's revenue and profit to approximate the turnover instead of referring to the firm's annual report or requiring information from the company according to Article 58(1)(a) of the GDPR. Thereafter, the DPA went on to conclude that an amount of 100 million NOK 'seems effective, proportionate and dissuasive', without further discussion.[80]

Basing the calculations of fines on turnover, there is no requirement that turnover be attributed to the processing of personal data. Neither is it a requirement that the infringement or non-compliance has led to profits or an economic advantage for the company. Article 83 of the GDPR does not distinguish between businesses that have data as their core asset and main revenue source and businesses where processing of personal data is a smaller part of their total revenue. However, if the controller has profited from the infringement, this should be taken into account when considering whether a fine should be imposed,[81] since economic gain should be compensated through measures that have a pecuniary component.[82] If we look to practice from competition law, the European Court of Auditors remarks that undue profits are not considered when calculating fines by the Commission nor national competition authorities. This is due to the difficulties in quantifying effects, requiring considerable resources.[83] We can only assume that assessing profits from personal data processing will be equally challenging for the DPAs.

The emphasis on turnover without regard to the economic benefits of personal data processing may lead to fines that are disproportionate. For example, in 2019 a German real estate firm was fined 14.5 million EUR for failing to delete data about former tenants. The annual turnover was 1.4 billion EUR, and the maximum fine would be 28 million EUR.[84] However, it can be questioned whether it is proper to use turnover to calculate the fine for a company whose main revenue comes from renting out apartments and not from processing personal data. The case was appealed to the court, which overturned the fine on procedural grounds, thus not entering into the issue of how the fine was determined.[85]

There are other examples of imposed fines that have been disputed in court. The court proceedings thus far do not support the notion of fines as an effective enforcement tool.[86]

An Austrian court overturned an 18 million EUR fine against the Austrian postal service on procedural grounds.[87] In Belgium, a court annulled a fine of 15,000 EUR, stating that the DPA should consider the full range of sanctions at its disposal before issuing a fine. In the court's view, imposing a fine for a first offence was not in accordance with the proportionality requirement of Article 83(1) of the GDPR.[88] In Germany, a regional court reduced a 9.55 million EUR fine against a telecom company to just 900,000 EUR. The court ruled that the fine was disproportionate and that too much emphasis had been given to the turnover at the group level. The violation was minor in nature and insufficient factors were taken into account in calculating the fine.[89] This

77 Datatilsynet (n 75) 7 and para 3.2.

78 Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (OJ L 182, 29.6.2013, pp 19–76.)

79 Data Protection Commissioner (n 58) 180–81.

80 Datatilsynet, 'Advance notification of an administrative fine' (24 January 2021) <www.datatilsynet.no/contentassets/da7652d0c072493c84a4c7af506cf293/advance-notification-of-an-administrative-fine.pdf>.

81 GDPR, Art 83(2).

82 WP29 (n 20) 16.

83 European Court of Auditors (n 29) para 17.

84 European Data Protection Board, 'Berlin Commissioner for Data Protection Imposes Fine on Real Estate Company' (5 November 2019) <https://edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_en>.

85 LG Berlin (526 OWi LG) 212 Js-OWi 1/20 (1/20). The Court stated that a person responsible for the infringements would have to be identified to impose an administrative fine. The Berlin public prosecutor's office has appealed the termination of the proceedings on behalf of Berliner Beuftragte für Datenschutz und Informationsfreiheit ('BlnBDI'); see press release 3 March 2021 <www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/20210303-PM-Deutsche_Wohnen.pdf>.

86 According to the European Data Protection Board, in the period May 2018 to May 2021, the total number of fine decisions by DPAs that were subject to a court appeal was 1037. Around a quarter of the decisions were annulled or modified by the courts, a quarter are still pending and the remaining half were confirmed by the courts, see European Data Protection Board (n 53) 20.

87 BvWG W258 2227269-1/14E. The Court noted that in order to impose a fine on a legal person, the DPA would have to identify a natural person whose culpable behaviour could be attributed to the legal person. This is similar to the abovementioned case from Berlin (n 85), and calls into question the compatibility between the procedures of art 83 of the GDPR and Member States rules on evidence and procedure.

88 Cour d'appell Bruxelles 2021/AR/163.

89 LG Bonn 29 OWi 1/20.

calls the standard calculation model of the German DPAs into question.

With the diverging practices of the DPAs in addressing non-compliance, whether fines are set and the size of fines, this can diminish the preventive and deterrent effect of the fines. The enforcement mechanisms will be of less value if applied differently by the DPAs and may eventually distort competition and lead to forum shopping.[90]

Lack of transparency

Both economic theory and responsive regulatory theory require transparency in the use of sanctions.[91] Without publicity and transparency about imposed fines, the deterrent effect of fines will be limited since there will be no signals of the cost of non-compliance. Knowledge of fines can also have an educational effect and lead to changes in behaviour. Without transparency, the regulation is unlikely to be effective.[92]

Transparency can take on special significance in GDPR enforcement. The assumption is that the GDPR will lead to harmonized practices throughout the Member States, despite the lack of harmonisation tools for enforcement of fines. Publication of decisions on fines can contribute to adjustments and harmonisations of practices, and also shed light on diverging practices. There is also limited case law concerning data protection fines both from Member State courts and the CJEU. The sanctions imposed by the DPAs through their administrative decisions and other enforcement mechanisms are therefore a significant source of practice. If these decisions are not made public, this can hinder transparency and obscure the effects of the GDPR.[93]

Transparency is subject to Member States' laws

However, the GDPR has no provision on publication of decisions by the DPAs.[94] This will be subject to Member States' regulation of whether and how decisions by the DPA can be published, which was also limiting public knowledge about enforcement of the former Data Protection Directive.[95] The result is a non-uniform manner of publication and a lack of transparency about the DPAs enforcement activities.

For example, the Norwegian DPA has issued several fines for unlawful access of credit information. Some of the decisions are published as press releases, others are filed as notable cases, while some are not available. Although the decisions are more or less the same in all cases, the publication of the number of infringement cases could be interesting, giving insight to the extent of malpractice, but also informing similar actors about enforcement activities. The decisions are based on long-term practice and former decision. However, in the guidance material on credit information, there is no information about what would constitute non-compliant behaviour or the current practice and level of fines.[96]

The lack of rules on transparency can also have other adverse effects. For example, in 2018 a case against Facebook by the UK DPA was settled out of court.[97] It has surfaced that the settlement included a gag-order for the DPA, thereby limiting the information the DPA could share with a parliament sub-committee on online harms and disinformation.[98]

The Luxembourg DPA publishes anonymized decisions on corrective measures,[99] while draft decisions on administrative fines are not published with reference to professional secrecy.[100] Whether this will also apply for final decisions is not clear. In October 2021, the privacy NGO 'NOYB – European Center for Digital Rights'

90 Alexander Dix, 'The Commission's Data Protection Reform After Snowden's Summer' (2013) 48(5) Intereconomics 268.

91 Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992) 35–52.

92 Graham Greenleaf, 'Responsive Regulation of Data Privacy: Theory and Asian Examples' in David Wright and Paul De Hert (eds), *Enforcing Privacy. Regulatory, Legal and Technical Approaches* (Springer 2016) 255.

93 Ibid.

94 Although art 59 of the GDPR requires the DPAs to draw up and make publicly available an annual report which 'may include a list of . . . types of measures taken', there is no obligation to provide a full list of enforcement decisions by the respective DPAs or to publish the decisions. By comparison, pursuant to art 68 of the Capital Requirements Directive, both the European Banking Authority and the competent authorities of the Member States are required to publish any administrative penalties. Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC Text with EEA relevance, OJ L 176, 338.

95 Christopher Kuner, *European Data Protection Law. Corporate Compliance and Regulation* (2nd edn, OUP 2007) para 1.81.

96 See Datatilsynet, 'Kredittvurdering' <www.datatilsynet.no/personvern-pa-ulike-omrader/kundehandtering-handel-og-medlemskap/kredittvurdering/>.

97 Information Commissioner's Office, 'Statement on an agreement reached between Facebook and the ICO' (30 October 2019) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/10/statement-on-an-agreement-reached-between-facebook-and-the-ico/>.

98 Natasha Lomas, 'Facebook's Secret Settlement on Cambridge Analytica Gags UK Data Watchdog' *Techcrunch* (26 January 2021) <https://techcrunch.com/2021/01/26/facebooks-secret-settlement-on-cambridge-analytica-gags-uk-data-watchdog/> . See also the recording from the UK Parliament Digital, Culture, Media and Sport Sub-committee on Online Harms and Disinformation (26 January 2021) <www.parliamentlive.tv/Event/Index/d4a948dd-b19a-4ece-adbe-8d84cfab09c5>.

99 See Commission nationale pour la protection de données, 'Décisions' <https://cnpd.public.lu/fr/decisions-sanctions.html>.

100 Commission nationale pour la protection de données (n 54).

('noyb') published a draft decision by the Irish DPA in a case concerning Facebook, to which noyb is a party as the representation of a complainant.[101] This prompted the Irish DPA to send a takedown request for breach of confidentiality duties.[102] Noyb referred to the Austrian General Administrative Procedure Act, § 17,[103] which does not limit the access and use of documents for a party in a case, while the Irish DPA is only partially subject to the Irish Freedom of Information Act 2014, cf. Schedule 1 Part 1.[104]

In contrast, the Belgium DPA publishes decisions to ensure transparency, but makes considerations of whether it is necessary to identify some or any of the parties for the sake of public interest.[105] The French DPA has also used publication of decisions as a form of 'name and shame', which was done in cases against Google and Microsoft. In addition to the punitive character of the publication, other motivations are to raise awareness amongst controllers and to inform the public.[106]

The lack of transparency by the EDPB

The EDPB keeps a register of final one-stop-shop decisions according to Article 60 of the GDPR, but due to national legal restrictions, none, or only some, decisions by the DPAs in Lithuania, the Netherlands, Spain, and some German states are included. There are also differences in Member State laws as to whether information about natural persons or legal persons is disclosed.[107] So while the one-stop-shop is promoted by the EDPB as a means to 'help individuals to stand up for their rights, no matter where they live in Europe',[108] the results of the DPAs' processing of the complaints are not necessarily available to the public.

Fines issued by the DPAs are not published in a structured way, and if and how information about cases ending in fines is published varies between DPAs. Neither does the EDPB provide a public overview of the fines and the infringements in questions, although their task is to harmonize practices. The EDPB started publishing short press releases of imposed fines by the DPAs for information purposes only in January 2020, but these are not endorsed by the EDPB nor express its views.[109] From the available information, it seems not to be the practice amongst DPAs to publish similar press releases commenting on fines being reduced or annulled following an appeal, which may give the impression that the enforcement activities of the DPAs are far more efficient and effective than they actually are. For example, the press releas about a fine of 14.5 million EUR to a German real estate firm, is still available on EDPB website, but with no later press release about the fine being annuled by the court, [110] In addition, since publication is at the discretion of the DPAs, it is a sample collection rather than a comprehensive overview of the enforcement practices of the DPAs.

Even though the EDPB stresses in its 2020 annual report that 'consistent enforcement of data protection rules is central to a harmonized data protection regime', the report itself only gives a few examples of decisions and offers no overview of eg the number of enforcement cases or decisions on administrative fines per DPA.[111] The most comprehensive overview from the EDPB is found in a report requested by the Committee on Civil Liberties, Justice and Home Affairs ('LIBE Committee') of the European Parliament with statistics on, *inter alia*, national and cross-border enforcement cases, number of decisions with a fine per DPA and number of fines that are subject to a court appeal.[112] The most up-to-date

101 noyb, 'Irish DPC greenlights Facebook's "GDPR bypass"' (13 October 2021) <https://noyb.eu/en/irish-dpc-greenlights-facebooks-gdpr-bypass>.

102 noyb, 'DPC "requires" noyb to take down documents from website' (15 October 2021) <https://noyb.eu/en/dpc-requires-noyb-take-down-documents-website>.

103 Allgemeines Verwaltungsverfahrensgesetz 1991 – AVG. StF: BGBl. Nr. 51/1991 (WV).

104 As stated by the Data Protection Commission: 'The DPC is subject to the Freedom of Information Act only in respect of records concerning the general administration of the Commission, and only specifically those created after 21 April, 2008. Consequently, records relating to, for example, the DPC's supervisory, regulatory, consultation, complaint-handling or investigatory functions (including case files), are not releasable under the Act' <www.dataprotection.ie/en/who-we-are/corporate-governance/freedom-information>.

105 The Belgian DPA has the power to 'décider au cas par cas de publier ses décisions sur le site internet de l'Autorité de protection des données', cf Loi du 3 Decembre 2017 portant création de l'Autorité de protection des données, art 95, §1er, 8º The decisions are published at Autorité de protection des données, 'Décisions de la Chambre Contentieuse' <www.autoriteprotectiondonnees.be/professionnel/chercher?q=&search_category%5B%5D=taxonomy%3Apublications&search_type%5B%5D=decision&search_subtype%5B%5D=taxonomy%3Adispute_chamber_substance_decisions&s=recent&l=25>.

106 Olivia Tambou, 'Lessons from the First Post-GDPR Fines of the CNIL against Google LLC' (2019) 5(1) European Data Protection Law Review 80, 82–84.

107 European Data Protection Board, 'Final One Stop Shop Decisions' <https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en>.

108 European Data Protection Board, 'The EDPB: Guaranteeing the same rights for all' <https://edpb.europa.eu/system/files/2021-06/2020_06_22_one-stop-shop_leaflet_en.pdf>.

109 European Data Protection Board, 'News' <https://edpb.europa.eu/news/news_en?news_type=2>.

110 EDPB (n 84).

111 European Data Protection Board, 'Annual Report 2020' para 6.1.4.1 <https://edpb.europa.eu/system/files/2021-06/edpb_aar_2020_final_27.05.21.pdf>.

112 European Data Protection Board (n 53).

overview of administrative fines is offered by a law firm, compiling publicly available data about decisions.[113]

The deterrent and preventive effect of fines can be questioned if the cases are not made known to the public or not reflected in guidance from the DPAs and the EDPB. It is also paradoxical that while transparency is a fundamental data protection principle, the enforcement activities of the DPAs are not subject to transparency requirements. Various national regulations on if, how and when administrative decisions can be made public add to the opacity of GDPR enforcement. The lack of transparency and overview can both diminish the educational effect of enforcement and negate the deterrent effect of fines and enforcement procedures.

Enforcement through other corrective powers

The lack of uniform enforcement has led to criticism from both privacy specialists and DPAs.[114] The European Commission has countered the criticism by stating that the success of the GDPR should not be measured by the number of fines, but by changes in behaviour. Instead of using fines, the DPAs are urged by the Commission to use other measures in the GDPR, such as temporary bans on the processing of data.[115]

This is also in line with the regulatory pyramid of responsive regulation theory, starting with dialogue and softer enforcement approaches before escalating to more punitive remedies when modest sanctions fail. Escalation through progressively more deterrent sanctions will often take the rational actor to the point where it becomes rational to comply.[116] The DPAs will require resources for both detection and assessment to be really responsive in their enforcement.[117] Harmonised practice amongst the DPAs will also be needed. If each DPA is applying different norms as to when to use dialogue and softer enforcement measures and when to escalate to more formal enforcement such as warnings and ultimately fines, then jurisprudence of enforcement of the GDPR will vary.

The power to impose fines has taken the spotlight, while the corrective powers of the DPAs in Article 58 of the GDPR are less communicated. The lack of transparency about the DPAs' practices of using corrective measures obscures the extent to which the DPAs use their powers and the effect these measures have on enforcement. For example, the Luxembourg DPA issued 140 corrective decisions from May 2018 to December 2019,[118] none of which are published on their website.[119] Whether these corrective measures have led to changes in culture, as pointed out by the DPA, is hard to assess when information is not available. The lack of visible enforcement activities draws criticism from data protection experts since the impression is that the Luxembourg DPA has shied away from enforcing the GDPR.[120]

The DPAs have the authority to, *inter alia*, impose temporary or permanent bans on further processing and to order the erasure of already collected and processed personal data.[121] A ban on processing can be an alternative or a supplement to imposing fines.[122]

For a company that relies on personal data for their business operation, an order to stop processing would be far more damaging than a fine. It could also potentially put them out of business. However, far more attention is given to the fines than the possibility of having to cease data processing and the deterrent effect this could have. Since the DPAs have various practices for disclosing information about their practice, the extent of the use of processing bans as an enforcement tool is not known.

For example, the French DPA's fine on Google of 50 million EUR is based on their assessment that Google lacked legal basis for the processing of personal data for personalized ads. Lacking legal basis, the processing will be illegal de facto, and the natural consequence is that the processing must be discontinued. However, the decision does not require Google to delete the related data and stop the processing.[123] A clear order to stop would

113 Enforcement tracker, provided by the German law firm CMS <www.enforcementtracker.com>.

114 Nicholas Vinocur, '"We Have a Huge Problem": European Tech Regulator Despairs Over Lack of Enforcement' *Politico* (27 December 2019) <www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605> .

115 Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation COM/2020/264 final, 5.

116 John Braithwaite, 'The essence of responsive regulation' (2011) 44(3) University of British Colombia Law Review 475.

117 Robert Baldwin and Julia Black, 'Really responsive regulation' (2008) 71(1) Modern Law Review 59.

118 Commission nationale pour la protection des données, 'Rapport annuel 2019' 56–57 <https://cnpd.public.lu/dam-assets/fr/publications/rapports/cnpd/rapport-annuel-%2B-annexes-2019-CNPD-BD.pdf>.

119 The first year of publication of decisions is 2021 (n 99).

120 Vincent Manancourt, 'Luxembourg Data Watchdog: "Big Penalties Not the Aim"' *Politico* (25 February 2021) <www.politico.eu/article/luxembourg-data-watchdog-big-penalties-not-the-aim-amazon-paypal/>.

121 GDPR, Art 58(2).

122 GDPR, Art 83(2).

123 Commission Nationale de l'Informatique et des Libertés, 'Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019

have had a more immediate effect on Google users than a fine.

If the purpose of the high fines in the GDPR was to rein in the large tech companies, it has not been successful. There are no major changes in behaviour or the business models of the companies, although data protection is duly mentioned and privacy policies are updated. In addition to diverging practices amongst the DPAs and the lack of consistent publication of their decisions, the deterrent effect of fines may be questioned.

The right to compensation for damages

Article 82 of the GDPR establishes the right to compensation for any person who has suffered material or non-material damages as a result of the controller's infringement of the GDPR.[124] The right can be exercised by bringing the case before the court, but can also be settled out of court between the parties.[125] The question of compensation is a matter between the affected person and the controller and does not involve the DPA. Neither is there a link between Article 82 and 83 of the GDPR, and the right to compensation is not dependent on or limited by the imposing of administrative fines.[126]

Since the proceedings will go before the national courts, the application of the rules will rely on national tort law. However, an important specification is that non-material damage should also be compensated. Since the purpose of the GDPR is to protect privacy rather than economic rights, a limitation of compensation to material damages would not have fulfilled the intention of the regulation.[127]

So far there is no case law from the CJEU relating to Article 82, nor based on the similar provision in the previous Data Protection Directive Article 23.[128] However, the Austrian Supreme Court has referred questions to the CJEU on whether an individual must have suffered harm for compensation to be awarded or if it is sufficient that provisions of the GDPR have been infringed. Also, the court poses the question if compensation for non-material damage presupposes the existence of a consequence of the infringement that goes beyond the upset caused by that infringement.[129]

A right in theory, but not in practice?

There is no overall overview of cases from the national courts, nor does the EDPB keep track of compensations to individuals. The extent of the application of Article 82 of the GDPR is therefore unclear. Cases from Member State courts provide some impressions on how the courts view the compensation of damages, and show divergences between the level of administrative fines and the compensation to affected individuals.

Two German courts acknowledged infringements of the Regulation, but the courts found the infringements to be minor[130] or that the person did not suffer a noticeable disadvantage that impaired personality-related matters.[131] No compensation was awarded in either case.[132] In other cases, the court has awarded compensation in the range of 300–1500 EUR.[133]

In the Netherlands, three of four cases awarding 500 EUR in compensation were overturned by the Court of Appeals, stating that a mere violation of fundamental rights does not automatically result in damages. The court found that the claimants failed to demonstrate that the threshold of harm was met.[134] In another case, the court established that the claimant had suffered anxiety and stress caused by the unlawful disclosure of personal data. The compensation was set at 250 euro.[135]

pronouncing a financial sanction against GOOGLE LLC' (21 January 2019) <www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf>.

124 For a discussion of whether 'any person' refers to both natural and legal persons, including a right for competitors to the controller to claim the right to compensation, see Tim F Walree and Pieter TJ Wolters, 'The Right to Compensation of a Competitor for a Violation of the GDPR' (2020) 10(4) International Data Privacy Law 346.

125 One of the few known cases is the H&M Service Centre in Nuremburg, which was fined 35.3 million EUR for unlawful processing of employees' data, and also agreed to pay an unknown amount of compensation to their employees. See EDPB, 'Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre' (2 October 2020) <https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en>.

126 For further discussions of the link between arts 82 and 83 of the GDPR, see Jane Reichel and Johanna Chamberlain, 'The Relationship Between Damages and Administrative Fines in the EU General Data Protection Regulation' (2020) 89(4) Mississippi Law Journal 667.

127 Gabriela Zanfir-Fortuna, 'Article 82: Right to compensation and liability' in Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020) 1173–74.

128 ibid 1170–71.

129 Case C-300/21: Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 12 May 2021—*UI v Österreichische Post AG. OJ C* 320, 9.8.2021, pp 25–26.

130 Oberlandesgericht Dresden Beschl. v. 11.06.2019, Az.: 4 U 760/19.

131 Amtsgericht Diez Schlussurteil v. 07.11.2018 - 8 C 130/18.

132 Sven Schonhofen, Friederike Wilde-Detmering and Alexander Hardinghaus, 'German Court Ruling: No Claim for Damages under Article 82 GDPR for Minor GDPR Violations' *Technology Law Dispatch* (21 August 2019) <www.technologylawdispatch.com/2019/08/in-the-courts/german-court-ruling-no-claims-for-damages-under-article-82-gdpr-for-minor-gdpr-violations/>.

133 Christoph Baus and others, 'GDPR Violations in Germany: Civil Damages Actions on the Rise' *Latham & Watkins* (18 December 2020) <www.jdsupra.com/legalnews/gdpr-violations-in-germany-civil-84570/>.

134 RaadVanState Uitspraak 201905087/1/A2.

135 Rechtbank Amsterdam 7560515 CV EXPL 19-4611.

In Austria, a regional court overturned a compensation of 800 euros. The court stated that although no serious violation of data protection rights is required to claim immaterial damages, there was no significant emotional damage or personal impairment to the plaintiffs. There should be a factual violation of rights, for example, exposure resulting from unlawful access to data. Not every GDPR violation would lead to compensation solely for general preventive reasons.[136]

Based on these cases, the right to compensation seems illusory. The courts set low damages or high thresholds for casualty. The requirement for proving damage is also considerably higher than the threshold the DPAs apply when issuing administrative fines. With compensations in the range of nil to 1500 euro, the risk of litigation is considerable. If a person pursues a case, with the procedural costs that will incur, the case is merely symbolic if awarded damages are as low as 250 EUR. Bringing a case before court will only be for the affluent or the resourceful.

The emergence of collective actions

Thus, we see the emergence of collective actions in the field of data protection. In the UK, the High Court has allowed the proceeding of a group litigation order against British Airways.[137] The case follows in the wake of a 20 million GPB fine imposed by the British DPA for the company's failure to protect the data of 400,000 customers caused by a cyberattack.[138] In a representative claim against Google LLC, the Court of Appeal considered that the claimant could recover damages for loss of control of their data, without proving pecuniary loss or distress.[139] However, the Supreme Court rejected the claim, stating that damages cannot be awarded without proof of financial damages and stress, thus the claim would not be suitable to proceed as a representative action.[140]

Similarly, collective action proceedings have been taken by a rights organization in the Netherlands against Oracle and Salesforce. The organization claims 500 EUR per person on behalf of the entire population. The total compensation is estimated at 5 billion EUR per company.[141]

The impact assessment of the GDPR pointed out that the threshold to use the right to compensation was high, and suggested the use of collective action as a measure.[142] This was not included in the GDPR, but Article 80 of the GDPR sets forth a right to representation where the data subject can mandate a non-profit entity to exercise the right to compensation on her/his behalf if provided for by Member State laws. Thus, rules on representation in damages proceedings are left to the Member States. However, in late 2020 a directive aimed at ensuring collective redress for consumers in all Member States was presented.[143] The Collective Redress Directive will include damage cases under the GDPR.[144] Unlike the GDPR, the Directive expressly requires Member States to allow qualified non-profit entities to launch representative actions for, *inter alia*, compensatory redress on behalf of groups of consumers. Although the Directive establishes the right to collective redress, the procedures will follow national legislations. Thus, the effect on compensations for data protection infringements will still depend on the national court's interpretation of tort law.

The misalignment between fines and compensation

Since the purpose of the GDPR is to defend the data protection of individuals, the lack of coherence between the use of fines as sanctions and the right to compensation may not sufficiently defend data protection rights. The non-alignment of the fines and the compensation leaves the persons behind. Natural persons, who the GDPR is said to protect, can be double losers, having their privacy infringed and then not be awarded damages.[145] The GDPR is promoted as a changemaker that ensures that individuals will be in control and own their personal data, but the mechanisms of the GDPR give them little room to enforce this right if they suffer damages.

136 OLG Innsbruck 13.2.2020, 1 R 182/19b. The case has been appealed to the Supreme Court, and the referral to the CJEU of questions relating to compensation mentioned in (n 129) concerns this case.

137 The High Court of Justice. Group Litigation Order Claim no [BL-2019-001146] <www.judiciary.uk/wp-content/uploads/2019/10/Weaver-ors-v-British-Airways-PLC-sealed-order.pdf>.

138 Information Commissioner's Office, 'ICO fines British Airways £20m for data breach affecting more than 400,000 customers' (16 October 2020) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/> accessed 7 October 2021. Since the infringement took place before the UK left the EU, the decision on the administrative fine followed the procedures of the GDPR.

139 *Lloyd v Google LLC* [2019] EWCA Civ 1599.

140 *Lloyd v Google LLC* [2021] UKSC 50. The case has been included since the proceedings started pre-brexit.

141 The Privacy Collective, 'Writ of Summons' (26 August 2020) <https://theprivacycollective.nl/wp-content/uploads/2020/11/Writ-of-Summons-English-translation-26-August-2020.pdf>.

142 Impact Assessment (n 13) 27, 36–37, 114–15.

143 Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, p 1–27).

144 Art 2 and Annex I (56) of the Collective Redress Directive.

145 Reichel and Chamberlain (n 126) 19.

In 2019, personal data of over 6 million individuals was disclosed on hacking forums following a security incident at the Bulgarian National Revenue Agency.[146] The Bulgarian DPA imposed a fine of 2.6 million EUR,[147] and the OECD suspended automatic information exchange with Bulgaria until information security was improved.[148] And while the DPA imposed a record fine on the National Revenue Agency, it pointed out that the affected individuals would have to resort to the procedures of tort law for compensation.[149] A person seeking damages was awarded 256 EUR by the court, but the decision was appealed by the National Revenue Agency.[150] The case is currently pending as the Supreme Administrative Court has referred questions to the CJEU concerning, *inter alia*, whether non-material damage should be interpreted broadly as to include the worries, fears and anxieties suffered by the data subject for possible future misuse of their personal data, entitling them to compensation for damages even if misuse has not been established or the person has not suffered any further harm.[151]

In a case from a Norwegian municipality previously mentioned in the section 'Effects of fines in the public sector', the use of a messaging app between schools and families resulted in the exposure of the whereabouts of children living at protected addresses. One mother changed her name. Another moved to a new address, and the children changed schools. The municipality helped out by buying the house at market value so the woman could buy a new house, but no compensation was awarded.[152] In addition to the costs incurred by moving, there were severe emotional damages caused by the fear of a violent ex-partner.[153] There is no doubt that the infringement caused both material and non-material damages. But for the woman wanting to put the incident behind her, it would be a further burden to take the case to court. In such a case, there can be a substantial gap between what the state is 'rewarded' through the fine and the economic compensation for the affected persons. The right to data protection may be defended as an idea, but without sufficient remedies for individuals to exercise their right to compensation.

Since the purpose of the GDPR is to protect the individual's right, and not the State, it could be considered whether fines can be used to compensate the individuals by including compensation in the fines[154] or by redistributing fines to the affected individuals instead of the state budget being the beneficiary. It may only provide a symbolic sum, but the compensation for damages for data protection infringements is already little short of symbolic.

Concluding remarks

There seems to be an assumption that the introduction of high fines will ensure compliance on its own, but as this article has shown, there is little evidence of the effect of mere imposition of fines. An analysis of the behavioural and deterrent effect of fines should be part of a future review of the GDPR.

Some remedies can easily be introduced to improve the enforcement mechanisms:

First, information about imposed fines should be made available in a transparent and accessible way, both by the national DPAs and the EDPB. Without making such information available to the public, a deterrent effect on others besides the perpetrator can hardly be expected.

Secondly, the use of fines on public authorities should be reconsidered. Depending on budget technicalities, the fines will only move money around within

146 The incident affected not only Bulgarian tax payers, but residents in other Member States and third countries whose data was included in information exchange between tax authorities. See *inter alia* Georgi Gotev, 'EU anti-fraud network EUROFISC hacked in Bulgaria' *EURACTIV* (26 July 2019) <www.euractiv.com/section/cybersecurity/news/eu-anti-fraud-network-eurofisc-hacked-in-bulgaria/>; Philip Baker, 'Editorial: Bulgarian Data Hack Provides a Timely Warning of Data Breaches to Come' (2019) 47(11) Intertax 908–09 <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\TAXI\TAXI2019092.pdf>. For an overview and timeline of the case, see Jearson Alfajardo, 'GDPR Violation Case Study: National Revenue Agency of Bulgaria' <http://cs.brown.edu/courses/csci2390/2020/assign/gdpr/ja43-nra.pdf>.

147 Commission for Personal Data Protection, 'Update on the undertaken inspection at the National Revenue Agency' (29 August 2019) <www.cpdp.bg/en/index.php?p=news_view&aid=1519>. Curiously, the decision by the Bulgarian DPA is not published on the EDPB website nor mentioned as a significant case in the EDPB annual report for 2019 or 2020.

148 OECD, 'Statement on the data breach in the National Revenue Agency of Bulgaria' (30 August 2019) <www.oecd.org/tax/transparency/documents/statement-on-the-data-breach-in-the-national-revenue-agency-of-bulgaria.htm>.

149 Commission for Personal Data Protection (n 147).

150 See GDPRhub, '**BAC** (Bulgaria) - 2606/2021' for a summary of the case <https://gdprhub.eu/index.php?title=%D0%92%D0%90%D0%A1_(Bulgaria)_-_2606/2021>.

151 Case C-340/21: Request for a preliminary ruling from the Varhoven administrativen sad (Bulgaria) lodged on 2 June 2021—*VB v Natsionalna agentsia za prihodite OJ C* 329, 16.8.2021, pp 12–13.

152 Even Norheim Johansen, 'Høyring om Vigilo-saka i Bergen: – Langt meir alvorleg enn venta' *NRK* (21 January 2020) <www.nrk.no/vestland/hoyring-om-vigilo-saka-i-bergen_-_-uforstaeleg-og-meir-alvorleg-enn-venta-1.14869344>.

153 Bergit Sønstebø Svendseid, 'Mor har fått valdsalarm etter at ekssambuar blei lagt til i skuleapp' *NRK* (23 October 2019) <www.nrk.no/vestland/mor-har-fatt-valdsalarm-etter-at-ekssambuar-blei-lagt-til-i-skuleapp-1.14751411>.

154 In South Korea, the DPA can order payment of compensation, although the payments are small and can be rejected by the parties who can take the case to court instead, see Greenleaf (n 92) 248.

the public sector and may reduce the service levels to the public. Other enforcement measures should be used instead. Alternatively, the fines could be used to compensate affected individuals instead of being allocated to the state budget.

Thirdly, the EDPB should issue guidelines for the imposition of fines, use of other enforcement tools and the calculation of fines to ensure harmonisation and consistency across Member States. Otherwise, there is a risk of undermining the intentions of the GDPR and giving incentives to controllers to establish in countries with lenient enforcement.

Fourthly, the DPAs should to a greater degree use their powers to ban processing or set strict terms for processing. For the data heavy companies, this will have a more immediate effect than fines.

Another remedy, which will require changes in the regulation, is to consider including compensation to the data subjects in the fine. The fines should not only be used as deterrence and punishment, but to actually remedy infringements inflicted on persons. In that way, the public will see that there is a price for infringements on their privacy.

The effect of the enforcement of fines and other corrective measures are still unknown. More research is needed on the effect fines have on behaviour and compliance with data protection legislation, taking into account how the protection of fundamental rights is different from market protection. Simply replicating fines from competition law may not have the intended effect due to the divergent natures of the legislations.

https://doi.org/10.1093/idpl/ipab024
Advance Access Publication 6 December 2021