# Feeling fine! Harmonisation and inconsistency in EU supervisory authority administrative fines

Received: 15th February, 2019

**Arye Schreiber**
is a dual-qualified lawyer, a data protection consultant and CEO of MyEDPO. Arye advises a broad range of clients, from early stage startups to public companies, NGOs, universities and government agencies. Arye has degrees in law, including MA (Cantab), LLM (University of London) and an MBA (Stanford) degree. In addition to his professional work in data protection, Arye has worked for over a decade in corporate law advising and representing tech corporations. Arye has published many articles in top tier law journals, and has been cited in the leading publications in privacy law. Arye lectures regularly in professional data protection fora, and holds CIPP/E and CIPM certifications, and is a Fellow of Information Privacy (FIP) of the IAPP.

Tel.: +44-203-870-3376; E-mail: arye@myedpo.com

**Abstract** GDPR has a stated goal of harmonisation in general, and of penalties in particular. This article demonstrates that under GDPR penalties, and especially fines, are inconsistently applied across EU member states, and that GDPR has left many of the most important topics relating to fines to member state legislation. The article starts by showing that the One-Stop Shop mechanism actually incentivises forum-shopping. Next, it is shown that the method of calculating fines is inconsistent and unsettled. Different language versions of GDPR lead to different conclusions as to how to calculate an undertaking's revenue, and the meaning of an undertaking is neither entirely consistent within GDPR itself, nor across member states. The role of regulators is likewise unclear, and in some member states the regulators do not even have the power to impose an administrative fine under GDPR. The role of non-regulators, such as data subjects and representatives of classes of data subjects similarly lacks consistency across member states. Public bodies are another area of disharmony between member states: the scope of applicability of GDPR to public bodies is a matter for member state legislation, and the outcomes are in fact different across member states. Additional areas discussed include: the responsibility and liability of directors and officers of a company; the enforceability of a contract for insurances against GDPR fines; choice of law clauses as governing data being processed under GDPR; and issuance of warnings prior to imposition of fines. In all these areas, GDPR itself and member state law is inconsistent and is far from harmonised. Finally, the role of the economic model of the infringing party in calculation of the applicable fine is unsettled, and is left to member states, and is therefore similarly at odds with a goal of harmonisation.

KEYWORDS: administrative fines, harmonisation, supervisory authorities, insurance, directors' liability, public bodies

## INTRODUCTION

The General Data Protection Regulation (GDPR) has introduced a new regime of administrative fines and other sanctions to EU data protection law and practice. Member state laws, supervisory authority

opinions and guidance, and the former Article 29 Working Party (WP29) guidelines, have all contributed to the development of the new powers vested in the supervisory authorities. This paper identifies some of the key emerging issues in this area: how and why fines are imposed, how they are assessed, how the risks of fines can be managed, who may be fined and more. As emerges from the paper, many of these topics are unsettled and, between various member states, inconsistent.

The GDPR's recitals lay out the legislative purposes of the GDPR. The Data Protection Directive 95/46/EC (the 'DPD') sought to 'harmonise' data protection (Recital 3) among member states, 'but it has not prevented fragmentation in the implementation of data protection across the Union' (Recital 9). The solution is in passing the GDPR; 'Consistent and homogenous application of the rules for the protection …of personal data should be ensured throughout the Union' (Recital 10). This includes not only the applicable law, but also the penalties for its violation: 'In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines' (Recital 150).

Even within the area of administrative fines under the GDPR, there are unresolved discrepancies that challenge the harmonisation goals of the GDPR, and threaten the predictability and effectiveness of administrative fines across member states. Ten such areas are briefly detailed now.

## EUROPEANISATION OF DATA PROTECTION AND THE RACE TO BE THE ONE-STOP SHOP

DPD Article 24 empowered member states to provide for sanctions for violations, but did not so much as mention fines. Administrative fines were levied under the member states' acts giving effect to the directive. Under the DPD fines, in so far as they were imposed at all, were localised. The maximum fine was set by the implementing laws in each member state. In Romania, the maximum fine was 500 million Lei, which, after the 2005 conversion, is 50,000 Romanian Lei, currently approximating €10,500. In Belgium, for example, it was €600,000, over 50 times greater than the Romanian maximum. The scope and effectiveness of administrative fines was entirely the prerogative of the member state, and indeed nothing in the DPD required administrative fines as such. The GDPR has made a dramatic departure from that model, grants supervisory authorities the power to issue administrative fines (with exceptions, discussed below), and moreover does so in a way that ostensibly promotes harmonisation across the member states. Under the GDPR, the maximal fines, the criteria for assessing fines, and even the scope of the infringements to which the fines relate, are Europeanised.[1] This is a part of the Europeanisation of data protection law under the GDPR. As noted by Lynskey,[2] the GDPR introduces several novel structures into the data protection regime; one that Lynskey focused on in particular is the administrative fines. Lynskey queried:

> once the consistency mechanism is engaged it is solely the lead authority that addresses a final decision to the data controller. It would also therefore seem logical to assume, although not expressly stipulated by the GDPR that it is solely that lead authority that can impose an administrative fine on the data controller (and therefore that each supervisory authority that is an addressee of the EDPB [European Data Protection Board] decision cannot impose an administrative fine on its own territory). Given the enhanced administrative fines foreseen by the Regulation, which are arguably now criminal in nature as a result of their severity, one could query whether the imposition of sanctions by multiple Member States would comply with the principle of *ne bis in idem*.

The GDPR does in fact address this, simply stating that 'the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice.'[3] In other words, the GDPR clearly answers Lynksey's question in the negative. How exactly that will be carried out in practice remains to be seen. This is particularly interesting as the supervisory authorities imposing an administrative fine collect the fine to the coffers of that member state, according to member state law. Thus, if the French authority imposes a €50M fine on Google (as is discussed below), that is a €50M boon to the French treasury. Perhaps the relevant supervisory authority extracts or justifies its budget based, inter alia, on its ability to finance itself, and more than finance itself, through the fines it imposes. This in turn will clearly lead to a rush to impose fines, especially on the biggest companies and deepest pockets, such as Google.[4] WP29 has rightly stated that a 'harmonized approach to administrative fines in the field of data protection requires active participation and information exchange among Supervisory Authorities.'[5] As a result, one can expect that some supervisory authorities will become known as more business friendly, others less so, with some jurisdictions thereby becoming preferred locations under the one-stop shop mechanism (see Recitals 127–128).

## THE NUMBER AND SIZE OF THE FINES

In its first year, the GDPR has dramatically increased both the number of investigations and also the magnitude of the fines, and this even with respect to infringements that took place under the DPD. Regarding the number of complaints and fines: according to the EDPB, in the 8 months since the GDPR came into force, there were 95,180 complaints filed with data protection authorities.[6] This represents a very significant increase in the number of complaints and investigations at the data supervisory authorities since the GDPR came into effect. For example, the Information Commissioner's Officer (ICO) has recorded a 133 per cent increase in the number of data protection cases it is currently handling,[7] compared with its pre-GDPR caseload. The number of fines issued in total is clearly not yet very high, because of the processing period of fines, but reports indicate that as of end of January 2019, there have been 91 fines imposed under the GDPR.[8]

Interestingly, the size of the fines has increased, and the GDPR seems to have had an effect even on fines issued under the DPD. For example, several files that were under investigation by the ICO under the DPD and Data Protection Act (DPA) 1998 were concluded after 25th May, 2018, when the GDPR was already in effect, and in two of those cases (Equifax[9] and Facebook[10]) the ICO imposed the maximum available fine under DPA 1998 — namely £500,000[11] — which it had never previously done. Regarding one of these fines, the Information Commissioner, Elizabeth Denham, said: 'We considered these contraventions to be so serious we imposed the maximum penalty under the previous legislation. The fine would inevitably have been significantly higher under the GDPR.'[12] This indicates that since under the GDPR, which was in force at the time this fine was imposed, the fine could have been potentially very much higher, the largest fine possible under the DPA 1998 no longer seems large, and was therefore imposed.

There are several open questions as to how fines are calculated under the GDPR. One ongoing argument between violators and authorities is the identity of the controller. Under the DPD, Facebook claimed that Facebook Ireland is the controller of data by Facebook in Europe; under the DPD, this view was promptly rejected by regulators and courts.[13]

Under the GDPR, Facebook's position is still less tenable, and the consequences for viewing Facebook, Inc., the US parent company, as the controller, or the undertaking in question, has very significant ramifications. GDPR Article 83(5) sets a maximum for an 'undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year.'[14] Recital 150 explains that an 'undertaking' could mean an entire corporate group, a position substantiated by Court of Justice of the European Union (CJEU) case law. Here, it is noteworthy that the GDPR itself refers and defers to EU competition law in the definition of an undertaking.[15] Yet this is a comparison that is far from obvious:

> Competition law seeks to avoid economic harm, namely a negative impact on the parameters of price, quality, choice and innovation which affect efficiency or consumer welfare. While data protection law can also prevent such economic harm (for instance, by tackling information and power asymmetries), this is not the sole objective of the data protection rules. These rules also seek to prevent harm to fundamental rights, such as privacy, non-discrimination and freedom of association. There are therefore many circumstances in which data protection and competition law will have no mutual influence. For instance, even if an undertaking's data processing policy complies with competition law, it may entail a violation of the right to privacy. Equally, not all competition law concerns are data protection concerns: for instance, personal data processing plays no role in many markets. It is also important to acknowledge that the methods employed in each field are distinct and, in this regard, data protection law appears more akin to consumer protection law.[16]

The relationship between competition law and data protection law is in its infancy, and there have been several major mergers in recent years, motivated in large part by the personal data sharing post-merger, giving rise to new opportunities to explore the relationship between these previously almost unrelated areas of law. For companies driven largely by personal data, the use or alleged misuse of personal data may provide an opportunity to test the relationship between competition law and data protection law. This was the case in Facebook's investigation by the German Competition Authority (GCA) for anti-competitive products, which essentially required users to agree to extensive data sharing — an alleged abuse of both data protection rules and of competition rules. The GCA ultimately found that various data protection violations could stand in their own right as anti-trust violations, since they were exclusionary and constituted anti-competitive abuse.[17] In this way, fines might be levied for anti-competitive behaviour, based entirely upon violations of the GDPR. At the very least, in such cases, the definition of 'undertaking' and other GDPR provisions drawing on competition law, will make sense.

Returning to the case of Facebook, its topline revenue globally in its previous financial year was US$40.653bn. Four percent of that sum amounts to US$1.623bn. That is approximately 3250 times the £500,000 that the ICO recently imposed on Facebook. As noted by Voigt and von dem Bussche,[18] the term 'undertaking' is used elsewhere in the GDPR with a narrower meaning; in Article 4(19), the GDPR offers the following definition: ''group of undertakings' means a controlling undertaking and its controlled undertakings.' In this definition, an 'undertaking' is clearly not a corporate group. In a conflict between the recital (Recital 150) and an article of the GDPR (Article 4(19)), the latter ought to be definitive. Yet both WP29 and supervisory authorities have already assumed the broader, indeed broadest, interpretation of 'undertaking' in the context of imposition of administrative fines.[19]

Likewise the definition of 'of the preceding financial year' is not settled. The French law, for example, provides 'chiffre d'affaires annuel mondial total de l'exercice précédent', which is a year, not necessarily a 'financial year' (Article 83(5)). This, in the present example, is very much to Facebook's advantage, as in the last calendar quarter of 2018, Facebook announced dramatically increased earnings, at an annualised rate of about US$67bn.

Thus both 'undertaking' and 'financial year' may be applied in a variety of ways, with no requirement for these to be harmonised. Moreover, member states may specifically reserve the right to determine the definition of 'undertaking', 'turnover' and 'financial year', which the UK has done, for example.[20]

Evidently, some of the most important definitions regarding administrative fines are not settled and need not be harmonised. Even the purpose of the fines is still largely discretionary, as discussed presently. The relationship between competition law and data protection law, enshrined in the GDPR, is in its earliest stages, and the way these affect each other beyond the definition of 'undertaking' may have very far-reaching effects on administrative fines and beyond.

## REGULATORS AND NON-REGULATORS AND THE PURPOSE OF ADMINISTRATIVE FINES

Data protection laws have existed for some time now, but there has long been a norm of corporations seeking 'to structure compliance by adapting to external mandates in ways that most easily achieve the appearance of legitimacy... focusing on easily visible indicators of compliance, rather than meaningful incorporation into firm decision making.'[21] In recent years, 'greater transparency around privacy failures has enabled nonregulators… to become credible enforcers.'[22] The GDPR has expanded the enforcement role of non-regulators in many ways. Most noticeably, data subjects have a host of access rights (GDPR Articles 12–23), with a resulting right to lodge complaints about data processors.[23]

Recital 129 sets out the powers that the GDPR gives regulators, such as 'investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons …to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing.' The GDPR thus puts special emphasis on the role of the natural person,[24] in the enforcement process.[25] Article 80 goes further and empowers data subjects to mandate a 'not-for-profit body… to lodge the complaint on his or her behalf', which is a roundabout way for groups to sue for their collective privacy rights,[26] or for interest groups to pursue GDPR violations that go against their group values. The non-profit NOYB, an acronym for None Of Your Business, founded by Max Schrems, quickly became perhaps the most prominent of such groups. Schrems was famously instrumental in pre-GDPR legislation,[27] but NOYB filed multiple complaints on 25th May, 2018, including one that led to the largest ever data protection fine. The influence that non-profit data protection advocacy groups will have on the data protection landscape and on fines is without precedent, since they had no standing under the DPD, but from the experiences of the first months of the GDPR, it appears that the non-regulators' influence will be considerable.

The roles of regulators are also not entirely settled. Bennet and Raab detail[28] the varied roles that data protection authorities fill, including ombudsmen, auditors, consultants, educators, policy advisors, negotiators and finally enforcers. But the

role of enforcers is far from obvious. In the Republic of Kosovo (not currently an EU member), for example, the data protection authority does not have the power to impose fines for violations of data protection law.[29] Some EU member states likewise do not. GDPR Article 83 states that administrative fines are to be 'effective, proportionate and dissuasive'. Yet after detailing the powers of supervisory authorities to impose administrative fines, the GDPR envisages a reality in which supervisory authorities do not have the power to impose a fine. Article 83(9) states:

> Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities.

Recital 151 explains that certain member states have not granted supervisory authorities the power to impose a fine. Notably, supervisory authorities in Denmark and Estonia do not have the power to impose an administrative fine under their respective national law. The Recital explains how the administrative fines may, nonetheless, be imposed in a consistent manner:

> The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.

The outcome here is that the GDPR instructs the independent courts of a member state how to issue misdemeanor fines and administrative fines. It remains to be seen to what extent a national court considers itself bound by the recitals of the GDPR. The roles of different member state supervisory authorities are thus clearly not harmonised and not settled.

## PUBLIC BODIES

Another important aspect of administrative fines yet to be clarified is how they will be applied to public bodies. This author is unaware of warnings and fines issued to public authorities, so far; however, aside from the practice of imposing fines on public authorities, there are some aspects of the GDPR left open on this matter, some matters of interpretation that are untested, and areas left to member state legislative discretion. Notably, there is member state discretion with respect to Article 83(7). The article states:

> Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

Different member states have reached very different conclusions in this regard. French data protection law applies the same administrative fine rules to public authorities as to non-public ones.[30] Others place limits: The UK DPA 2018 has reserved for the secretary of state the power to determine whether and to what extent administrative fines may be imposed on public authorities.[31] The Irish DPA 2018 specifically empowers the supervisory authority to impose

administrative fines on public authorities, but limits the fines to €1m.[32] In some member states this was a hotly debated topic; in the House of Commons, it was determined that certain public authorities, such as parishes, would be excluded from the definition of 'the term "Public Authority" under GDPR'.[33] In the Danish law's legislative history, this matter was likewise a subject of considerable wrangling:

> One of the main topics discussed with regards to the adaption of the GDPR to the Danish legal system was whether or not public authorities should be subject to fines. The Ministry of Justice had not decided on this in the first draft of the Data Protection Act that was published for public consultation. However, just before the first parliamentary reading the Ministry of Justice added a section in § 41 of the Data Protection Act that provides that public authorities can be sanctioned with fines as well as private actors. Under the first reading in Parliament, the Minister of Justice, Søren Pape Poulsen, stated that the government found it reasonable and fair to sanction public authorities as well as for private actors for infringements of the Data Protection Act and the GDPR.[34]

As is apparent from this small sample of approaches, different member states often do not have a settled jurisprudence on this, and there is no harmonised approach. There are also some interpretive matters that remain open.

Returning to Article 83(7): 'each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State'. How is this sentence to be read? The word 'public' clearly qualifies 'authorities', but does it qualify 'bodies'? In other words, does this section apply to both public authorities, and to bodies, established in a member states, or does it apply to public authorities and public bodies established in that member state? Recital 154, for example, states: 'The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents.' There, it is made clear that 'public' does not qualify 'bodies'.[35] Conversely, Article 41(6) states that 'This Article shall not apply to processing carried out by public authorities and bodies'. In that case, it is clear that public qualifies 'bodies'.[36] At any rate, one wonders what the point of fining a public body could be. The administrative fines are collected by the state, which has the power to promptly return the fine to the public body, and the matter would be more complicated where quasi-national authorities, privatised national services, state-managed companies, local authorities and so on would be concerned. Member state jurisprudence and legislation differs in this area, and so there is little hope or aspiration for harmonisation.

## INDIVIDUALS AND OFFICERS

Under the GDPR, any act of an employee, presumably acting in their capacity as such, can be attributed to the employer.[37] More complex is the imposition of fines on individuals for corporate violations. Some member states specifically authorise imposing sanctions on directors and officers of violating legal entities. For example, the Irish Data Protection Act 2018 provides that where a corporate entity has committed an offence, and it is proven to have been with the 'consent or connivance of, or to be attributable to any neglect on the part of' a director, manager, company secretary, officer or a person purporting to be one of those, then that person may be found guilty of and may be punished for that offence as if it were they who committed it.[38] UK law similarly provides that 'The director, manager, secretary, officer or person, as well as the body corporate, is guilty of the offence and liable to be proceeded against and punished accordingly.'[39]

The UK Supreme Court ruling in *Vestergaard* is interesting in this regard.[40] The case involved former employees of Vestergaard who started a competing business. One of the employees took along with him some trade secrets of Vestergaard and used them at the new business — a breach of his duty of confidence to this former employer. Another of the employees demonstrated that she had no knowledge, nor constructive knowledge, of the misappropriation of the trade secrets, and it was found that she was therefore not in violation of her duty of confidence. The case is pertinent to the GDPR in light of the requirements of Article 28(3)(b) that a processor must ensure 'that persons authorised to process the personal data have committed themselves to confidentiality.' Constructive knowledge, meaning that the person ought to have known, may be sufficient for a finding of breach of a duty of confidence. In *Vestergaard*, the courts were not in agreement, and in the future one may expect robust deliberation as to the role of constructive knowledge, vicarious responsibility and the boundaries of executive responsibility under the GDPR. These cardinal questions are within the realm of member state law, introducing further lack of harmonisation in the law and additional motive for forum shopping of sorts.

## INSURANCE

Insurance is an additional area that has potential to influence greatly the world of administrative fines.[41] Put succinctly, administrative fines generally have a criminal law character, and they are intended to dissuade deviant behaviour. Yet, where a party has insured against such fines, that takes the sting out of the supervisory authority's tail.[42] Where there is insurance against fines, the fines will generally fail their essential purpose, calling into the question the point, if any, of imposing them. For this reason, in many states there is a public policy that restricts the validity of insurance against regulatory fines. Where insurance is valid, the premia paid to insurers essentially means that one perpetrator's fine is spread across many parties — the insurer's or underwriter's clients. The preparatory work of the insurers means that they ought to best understand the risks of each party, and can set the premium for each insured party to match their chances of being fined. Thus, in some respects the fines may be viewed as being amortised. But the public policy remains widespread across member states, that regulatory fines ought not to be insurable. Insurance of fines under the GDPR have not yet been the subject of case law, to the author's knowledge, and in the meantime there remains a public policy challenge to such insurance, meaning that this contract may be in violation of public policy, and may be found to be unenforceable.

One review of the area suggests that only Finland and Norway (the latter is not an EU member, but an European Economic Area (EEA) member) enable insurance against GDPR fines.[43] In Finland, this is qualified by the *mens rea* such that deliberate or gross negligence violations are not insurable; for some EU member states, the insurability of GDPR fines is unclear; and for most EU member states, GDPR fines are uninsurable. This entire area of law remains completely within the remit of member states, and is as yet untested.

## CHOICE OF LAW

The factors listed above, such as director liability and the insurability of GDPR administrative fines, may subsequently influence the one-stop shop doctrine and the almost inevitable forum shopping. Under DPD, there was a significant forum shopping problem, and this ought to have been largely ameliorated by the broad and direct applicability of the GDPR's provisions. Nevertheless, insurability and director liability are matters for local law, and may therefore play into both choice of

law provisions and lead supervisory authority election. Brkan wrote, of the state of choice of law provisions under the DPD:

> The current doctrine and practice is divided regarding the question whether the parties to a contract can freely choose data protection law that is applicable for processing of data and for data protection breaches in a framework of this contract.[44]

She concludes that, in contrast with DPD's Article 4(1), the GDPR 'unifies EU data protection rules and hence no longer contains an overarching conflict-of-law provision.'[45] It is true that there is no overarching provision, but there is certainly a strong interest for parties to choose their applicable law.

WP29 has stated emphatically: 'The GDPR does not permit "forum shopping".'[46] Indeed, with respect to identifying the lead supervisory authority, there is a mechanism in place to ensure that the identity of the lead supervisory authority follows the jurisdiction of the main establishment. It appears, however, that this will not generally affect contractual terms. In other words, where a data protection agreement states that the laws of, say, Finland, will govern, then even if the lead supervisory authority of the processor and controller is the Commission nationale de l'informatique et des libertés (CNIL) in France, the contract, its terms, interpretation and so on ought to be governed by Finnish law, or at least by the Finnish data protection law.

Choice of law issues may be expected to raise some interesting challenges of this kind for supervisory authorities and courts, and it remains to be seen how they are to be contended with.

## WARNINGS

Several supervisory authorities have issued various forms of warnings or notice to alleged violators of the GDPR. Indeed, the GDPR generally encourages or envisages a warning being issued prior to a fine being imposed,[47] and the published notices give some useful insight into the supervisory authorities' aims in the fines that may follow the warnings. The warnings offer some insight into the factors that may be considered by the supervisory authorities. The general factors are listed in the GDPR, but each supervisory authority may place the emphasis where they see fit.

There has been at least one case of a supervisory authority issuing a warning and notice to a non-EU entity. The UK's ICO issued a notice to AggregateIQ (AIQ), a company providing data and data analytics in connection with political campaigns. According to the ICO, AIQ had violated the lawfulness, transparency and fairness principles, and the purpose limitation and data minimisation principles. AIQ was issued with a warning,[48] and the ICO specifically considered whether 'the failure has caused or is likely to cause any person damage or distress', as required by section 150(2) of the DPA 2018. This introduces an additional element, in this case based on local law, of 'distress', as a factor in possible imposition of sanctions.[49]

In July 2018, CNIL issued warnings[50] to Teemo, Inc. and Fidzup SAS, two companies allegedly collecting and retaining geolocation data, and this is in contravention of the GDPR. The companies were warned to obtain consent and correct other data practices within a period of 3 months. In both cases, the companies had developed SDK – software development kits. This is a module of code that other app builders could include in their apps, and which collects various data — returning it to the app builders and owners, but also to the authors of the SDK, in this case, Teemo and Fidzup. Teemo's SDK collected geolocation data; Fidzup's enabled sending a targeted advertisement to any user who was near a Fidzup point of sale installation. CNIL found the alleged consent of the users

inadequate, the data retention excessive and information that ought to have been provided to the data subjects had not been provided as required. In this case, the violators were given 3 months to correct the situation; that appears to be more than enough time, and it seems from the CNIL notice that if indeed they apply the necessary fixes, they will be saved from a fine.

In addition to formal data protection authority warnings, there may be a variety of notices and warnings prior to a formal complaint and investigation. Microsoft was the subject of a fairly damning review, commissioned by the Dutch Ministry of Justice, of the data protection practices among offices of a major Microsoft customers — government institutions in Holland.[51] The review found several high-risk clusters of activity, noting that Microsoft's services as used by the Dutch government, reflect a lack of transparency, unlawful storage of special categories of personal data, lack of purpose limitation and more. This has acted as a warning to Microsoft, but has the potential for massive fines. The goal of making Microsoft services compliant may be better served in this case by the warning than by the fines.

It therefore appears, thus far in the evolution of administrative fines, that warnings ought to be taken very seriously, and that a full and effective response to a warning may entirely avoid a fine. The warnings issued may further elucidate likely considerations in the imposition of a fine, and generally offer a chance to rectify a violation, with exceptions, as discussed presently.

## FINES IN PRACTICE

To date, supervisory authorities have imposed only a handful of fines under the GDPR. There are important indications of the various elements considered by the supervisory authorities, and these are elaborated on presently.[52] To that end, several instances are briefly discussed below.

The first fine issued under the GDPR and the new Bundesdatenschutzgesetz (BDSG) was issued by Landesamt für Datenschutzaufsicht (LfDI), the data protection authority of Baden-Wuertemberg.[53] The case involved a social dating site that had stored user passwords in clear text, inadequately protected the data and then suffered a breach. The LfDI emphasised that the company's cooperation and transparency in the investigation was exemplary, as well as its responsiveness to the LfDI's demands. These expressly motivated the LfDI to impose a relatively modest fine of €20,000. The commissioner, Dr Stephan Brink, said that the LfDI was not in a competition to impose the highest possible fine, but was tasked with protecting the rights of data subjects.

Another early GDPR fine was issued by the Austrian data protection authority. The Austrian Datenschutzgesetz, the data protection act, in section 11 specifically states that first-time infringements will generally be met with a warning.[54] Notwithstanding that, in the case of a betting establishment, the owner had installed CCTV which was filming public spaces outside the establishment. It was found that the business did not keep records of processing, did not delete data and had no justification for the same, and it did not give notice that there was video surveillance in place.[55] The fines for these infringements were €2400 for the first and €800 for the latter three, totalling €4800.[56]

More significant fines were levied in the case of a Portuguese hospital. Centro Hospitalar Barreiro Montijo[57] was fined €400,000, a very significant sum. Of this, €150,000 was for not adhering to the data minimisation principle; another €150,000 was for not putting in place appropriate technical and organisation measures to protect the data from unlawful access; and €100,000 for lack of data security measures commensurate with the risks of the data. Of particular interest is the first

of these infractions: the hospital had 985 users defined as 'doctors' in its central data system, but only had 296 actual doctors on the staff. Several considerations played into the relatively harsh fines imposed by the Portuguese data protection authority, the Commission nationale pour la protection des données (CNPD). One was the sensitivity of the data, namely medical data. Another was that the hospital did not report the breaches, but an investigation was begun after media reports of data mismanagement. The apparent willful neglect of the hospital with respect to data security and the knowing and egregious lack of data minimisation, were central in the imposition of this very significant fine. This fine underscores the *mens rea*'s role in determining the size of the fine imposed. Shortly after this case, another GDPR fine was imposed that was two orders of magnitude greater, and which depended less on the *mens rea* of the perpetrator and more on its economic model, and is discussed next.

## THE VIOLATOR'S ECONOMIC MODEL

On 21st January, 2019 the French supervisory authority, CNIL, imposed the largest data protection fine yet, that of €50m, on Google.[58] The main violations by Google were that the consents obtained for their Android operating system were invalid, principally on account of the lack of specificity, with one act of consent for Android ultimately leading to personal data being used in Google Search, YouTube, Google Home, Google Maps, Playstore, Google Pictures and more. As a result, Google was actually collecting a vast amount of personal data with no lawful basis whatsoever, in violation of the GDPR. Google was thus essentially flaunting several of the central tenets of the GDPR, and did so with respect to a very large number of data subjects. In explaining the magnitude of the fine, CNIL noted (the following is an unofficial English language translation):

> The amount and the publicity of the fine, are justified by the severity of the infringements of the principles of transparency, information and consent; the violations are continuous not limited in time; and the economic model of the company is partly based on the ads' personalization.

In other words, several aspects played into the severity of the fine. Most notably, the severity of the violations of two pillars of data protection, that is, lawful processing and transparency. Likewise, the massive number of data subjects affected was an important factor. More interestingly here, is the last sentence quoted above: 'the economic model of the company is partly based on the ads' personalization.' This is in line with the expectation of Recital 149 that member states will legislate for penalties that include 'deprivation of the profits obtained through infringements' of the GDPR. French law did in fact previously include such a provision:

> The amount of the financial penalty provided under Article 45 Section I shall be proportional to the severity of the breaches committed and to the profits derived from said breach.'[59]

The amended French data protection law does not, however.[60] Rather, the French law simply references GDPR Article 83 for criteria that may be considered in imposing a fine.[61] Article 83(k) states: 'any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.' In this case, it was enough for CNIL to state that Google's business model involves making money from personalised advertising, to establish that there was an aggravating factor. In other words, CNIL

was not trying to impose an account of profits, but viewed the business model as an aggravating factor. Even if French law had in fact provided for an accounting of profits, presumably CNIL would still try to avoid demanding an account, which would make the case inordinately complicated and may ultimately show that the profit from the infringing act was very much less than the fines.

Recital 149 allows for member states to grant supervisory authorities the power to impose an account of profits for breaches of the GDPR. In the EU, Article 13 of the 2004 Enforcement Directive provides for an account of profits as a remedy in intellectual property cases. This has not typically included breach of confidence.[62] The remedy of account of profits is generally available in intellectual property violations, but the Court of Appeal in *Vestergaard* indicated that Article 13 of the Enforcement Directive applied.[63] This is connected with a broader issue — that of the 'propertisation' of data.[64] As data are increasingly viewed as property, data protection rights will increasingly be viewed as intellectual property rights. The propertisation of data, the availability of an account of profits as a remedy and the use of the perpetrator's economic model as an aggravating factor in assessing a violation, are all factors largely dependent on member state law, and have yet to be clarified in the context of the GDPR.

## CONCLUSIONS

It has been shown above that though the GDPR sought to harmonise data protection laws generally and administrative fines in particular, there remain many considerations and factors that are untested, unsettled and generally open to member state law. These include warnings, the role of regulators and non-regulators such as public interest groups, choice of law, insurability, directors' and officers' liability and the use of the perpetrators economic model in consideration of fines. These and other factors lead to a conclusion that although the situation may be improved as compared with the DPD, the GDPR most certainly has not yet harmonised EU data protection law, and especially the fines imposed under the GDPR.

## References and Notes


1. Giurgiu, A. and Larsen, T. A. (2016) 'Roles and powers of national data protection authorities', *European Data Protection Law Review*, Vol. 2, No. 3, pp. 342–352.
2. Lynskey, O. (2016) 'The Europeanisation of data protection law', Cambridge Yearbook of European Legal Studies, Vol. 19, pp. 252–286; see p. 274 for quote.
3. Recital 149.
4. One may thus contemplate the following: if the fines are imposed based on pan-European criteria, and on the basis of infringement across the EU, ought the fines therefore not be shared across the relevant member states, say in proportion to the number of relevant data subjects in each, or perhaps by some other mechanism between member states?
5. Working Party 29 Opinion 253, adopted 3rd October, 2017: Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679.
6. EU Commission, https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf (accessed 10th May, 2019).
7. Khanna, M. (2018) '2018 GDPR Study', Prosults Ltd, available at: https://iapp.org/media/pdf/resource_center/2018_GDPR_Study.pdf (accessed 10th May, 2019).
8. DLA Piper (2019) 'GDPR data breach survey', February, DLA Piper LLP, available at: https://www.dlapiper.com/en/uk/insights/publications/2019/01/gdpr-data-breach-survey/ (accessed 10th May, 2019).
9. Denham, E. (2018) ICO, available at: https://ico.org.uk/media/2259808/equifax-ltd-mpn-20180919.pdf (accessed 10th May, 2019).
10. Denham, E. (2018) ICO, available at: https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf (accessed 10th May, 2019).
11. ICO (2018) 'ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information', 25th October, available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/ (accessed 10th May, 2019).
12. Denham, E. (2018) See her interview here: https://vimeo.com/296670132/d04544e679 (accessed 10th May, 2019).

13. Van Canneyt, T. (2015) 'The Belgian Facebook recommendation: How the nomination of a single EU Data controller is under fire', 20th May, available at: https://privacylawblog.fieldfisher.com/2015/the-belgian-facebook-recommendation-how-the-nomination-of-a-single-eu-data-controller-is-under-fire (accessed 10th May, 2019). See discussion in Bu-Pasha, S. (2017) 'Cross-border issues under EU data protection law with regards to personal data protection', *Information & Communications Technology Law*, Vol. 26, No. 3, pp. 213–228.
14. The French law, for example, provides 'chiffre d'affaires annuel mondial total de l'exercice précédent', which is a year, not necessarily a 'financial year' (Article 83(5)). This, in the present example, is very much to Facebook's advantage, as Facebook announced dramatically increased earnings for the last calendar quarter of 2018, at an annualised rate of about US$67bn. Note that member states may reserve the right to determine the definition of 'undertaking', 'turnover' and 'financial year'; see, for example, UK DPA 2018 s.159.
15. As noted by WP29 Opinion 253, footnote 4. Recital 150 refers to Articles 101 and 102 of the Treaty on the Functioning of the European Union; those provisions provide a wide interpretation of 'undertaking', based on competition law precedent. See Voigt P. and von dem Bussche, A. (2017) 'The EU General Data Protection Regulation (GDPR)', Springer, Cham, Switzerland, pp. 212–213; Golla, S. (2017) 'Is data protection law growing teeth? The current lack of sanctions in data protection law and administrative fines under the GDPR', *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 8, No. 1, pp. 70–78, see p.76 for discussion and sources on the meaning of 'undertaking'. That article pre-dates WP29, and subsequent fines, all of which support the broadest interpretation of undertaking as, essentially, a corporate group.
16. Costa-Cabral, F. and Lynskey, O. (2017) 'Family ties: The intersection between data protection and competition in EU law', *Common Market Law Review*, Vol. 54, No. 1, pp. 11–50, para 2.2. See extensive discussion in Santos Silva, A. R. (2017) 'Towards the incorporation of privacy in EU competition law: How data protection harms can reduce the quality of goods and services', Master's thesis, Tilburg University.
17. Colangeo, G. and Maggionlio, M. (2018) 'Data accumulation and the privacy–antitrust interface: Insights from the Facebook case', *International Data Privacy Law*, Vol. 8, No. 3, pp. 224–239.
18. Voigt and von dem Bussche, ref. 15 above.
19. Golla, ref. 15 above.
20. UK DPA 2018 s.159.
21. Bamberger, K. A. A. and Mulligan, D. K. (2015) 'Privacy on the ground', MIT, Cambridge, MA, p. 28.
22. *Ibid*., p. 230.
23. A right that data controllers must specifically bring to the attention of the data subject; see Articles 12(4), 13(2)(d), 14(2)(e), 15(1)(f), and with respect to BCRs 47(2)(e).
24. In this recital the text refers to a 'natural person', but in Article 57(1)(f) the regulation refers to a 'data subject'. An important difference, but one which is not the focus of this paper.
25. See further Recital 141.
26. See at length Taylor, L., Floridi, L., and van der Sloot, B. (eds) (2017) 'Group privacy', Springer, Cham, Switzerland.
27. *Schrems v Data Protection Commissioner* [2014] IEHC 310 (18 June 2014).
28. Bennett, C. J. and Raab, C. D. (2006) 'The governance of privacy', MIT, Cambridge, MA, pp.133–143. More recently, and a comparison of the roles of DPAs in the DPD and GDPR compared: Giurgiu, A. and Larsen, T. A. (2016) 'Roles and powers of national data protection authorities' *European Data Protection Law Review*, Vol. 3, pp. 342–352.
29. See discussion in Zenjnullahu, N. (2016) 'Imposition of monetary sanctions as a mechanism for protection of personal data', *European Data Protection Law Review*, Vol. 1, pp. 80–90.
30. Loi Informatique et Libertes Act No. 78-17, 6 January 1978. Article 3.
31. DPA 2018 s.56(b)(1).
32. Irish DPA 2018, s.141.
33. UK DPA 2018 s.7, see Hansard, 9th May, 2018, column 790.
34. Overby, T. (2018) 'The Danish adaptation of GDPR', June, available at: https://blogdroiteuropeen.com. First reading of the Data Protection Act in Parliament, available at: http://www.ft.dk/samling/20171/lovforslag/L68/BEH1-20/forhandling.htm (Danish) (accessed 10th May, 2019).
35. Likewise in Recital 108, and Recital 158.
36. Likewise Recital 92.
37. See 'Short Opinion 2 – Supervisory Sanctions' of the German Data Protection Conference – DSK, available at: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/kurzpapiere/DSK_KPNr_2_Sanktionen.pdf (accessed 10th May, 2019).
38. Irish DPA 2018, s.146.
39. UK DPA 2018, s.198.
40. *Vestergaard Frandsen v Bestnet Europe* [2013] UKSC 31.
41. Baker, J. (2019) 'Data breach insurance: A three-part problem', IAPP, The Privacy Advisor blog, 29th January, available at: https://iapp.org/news/a/data-breach-insurance-a-three-part-problem/ (accessed 10th May, 2019).
42. There seems little punitive element in administrative fines under the GDPR, but member state laws add criminal stigma, prison sentences and other traditional elements of criminal sanction.
43. 'The price of data security: A guide to the insurability of GDPR fines across Europe', DLAPiper and Aon report, May 2018, available at: https://www.aon.com/attachments/risk-services/Aon_DLA-Piper-GDPR-Fines-Guide_Final_May2018.pdf (accessed 10th May, 2019).

44. Brkan, M. (2016) 'Data protection and conflict-of-laws', *European Data Protection Law Review*, Vol 2, No. 3, pp. 324–341.
45. *Ibid*., p. 340.
46. WP29 244 (2016) 'Guidelines for identifying a controller or processor's lead supervisory authority', 13th December, p. 7.
47. Recital 151, Article 58(2)(a).
48. Denham, E. (2018) Information Commissioner, Enforcement Notice, available at: https://ico.org.uk/media/action-weve-taken/enforcement-notices/2260123/aggregate-iq-en-20181024.pdf (accessed 10th May, 2019).
49. The First Tier Tribunal (Information Rights) overturned ICO's fine in *Scottish Borders Council v Information Commissioner* [2013] EA/2012/0212, since it was found that there was not a likelihood that harm would materialise. See discussion in Ceross, A. (2018) 'Examining data protection enforcement actions through qualitative interviews and data exploration', *International Review of Law, Computers & Technology*, Vol. 32, No. 1, pp. 99–117.
50. CNIL, available at: https://www.cnil.fr/fr/applications-mobiles-mises-en-demeure-absence-de-consentement-geolocalisation-ciblage-publicitaire (accessed 10th May, 2019).
51. Nas, S. and Roosendaal, A. (2018) 'DPIA Diagnostic Data In Microsoft Office Proplus', Ministry of Justice and Security for the benefit of SLM Rijk (Strategic Vendor Management Microsoft Dutch Government), available at: https://regmedia.co.uk/2018/11/16/microsoft-office-gdpr-fail.pdf (accessed 10th May, 2019).
52. There are fairly comprehensive surveys of fines and actions under DPD – see Ceross, ref. 49 above; less so under the GDPR, owing to the short time that the GDPR has been in force.
53. 'Kooperation mit Aufsicht macht es glimpflich' (unofficial translation: 'Cooperation with the Supervisory Authority makes it easy'), 2018, available at: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/11/LfDI-Baden-W%C3%BCrttemberg-verh%C3%A4ngt-sein-erstes-Bu%C3%9Fgeld-in-Deutschland-nach-der-DS-GVO.pdf (accessed 10th May, 2019).
54. As does the UK Data Protection Act 2018, s.115(9). See also Austrian Federal Act for the Protection of Individuals with regard to the Processing of Personal Data (Data Protection Act — DSG), available at: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597 (accessed 10th May, 2019).
55. Austrian data protection authority, Datenshutz behörde ('DSB'), available at: https://www.dsb.gv.at/documents/22758/116802/Straferkenntnis+DSB-D550.038+0003-DSB+2018.pdf/fb0bb313-8651-44ac-a713-c286d83e3f19 (accessed 10th May, 2019).
56. Compared with a merely symbolic fine of 1500 CZK (less than €100) issued in 2007 by the Czech data protection authority against Rynes. See at length the appeal to the Czech court: František Ryneš v Úřad pro ochranuosobníchúdajů (Office of the Protection of Personal Data), 113/2012, and of course the CJEU appeal of the same name, which overturned the court's annulling the fine; František Ryneš v Úřad pro ochranuosobníchúdajů C212/13.
57. Menezes Monteiro, A. (2019) 'First GDPR fine in Portugal issued against hospital for three violations', IAPP, available at: https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/ (accessed 10th May, 2019).
58. CNIL, https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (accessed 10th, May, 2019).
59. Loi no. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, Article 47.
60. Ordonnance no. 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi no. 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi no. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.
61. Article 20(3)(7).
62. See discussion in Johnson, P. (2013) '"Damages" in European law and the traditional account of profits', *Queen Mary Journal of Intellectual Property*, Vol. 3, pp. 296–306. In the EU, this is mandated by Article 13 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.
63. *Vestergaard Frandsen v Bestnet Europe* [2009] EWHC 1623 para 56, per Jacob LJ.
64. See at length: Evans, B. J. (2011) 'Much ado about data ownership', *Harvard Journal of Law and Technology*, Vol. 25, No. 1, pp. 69–130. More generally, on the propertisation of data protection, see Pearce, H. (2018) 'Personality, property and other provocations', *European Data Protection Law Review*, Vol. 4, No. 2, pp. 190–208; Schreiber, A. (2009) 'Privacy: Proprietary or human right?', *Intellectual Property Quarterly*, No. 1, pp. 99–138.