A point for setting administrative fines under the GDPR


WINSTON MAXWELL
Partner, Hogan Lovells, Paris

CHRISTINE GATEAU
Partner, Hogan Lovells, Paris

Article 83 of the GDPR[1] provides for two levels of administrative fines: a lower level - maximum of €10 million or 2% of the global turnover - for violations relating to record-keeping, data security, data protection impact assessments, data protection by design and default, and data processing agreements; and a higher level - maximum of €20 million or 4% of the global turnover - for violations relating to data protection principles, the legal basis for processing, information to data subjects, the prohibition of processing sensitive data, denial of data subjects' rights, and data transfers to non-EU countries.

In addition to setting two levels of administrative fines, Article 83 of the GDPR provides criteria that national supervisory authorities must apply when setting administrative fines. On 3 October 2017, the Article 29 Working Party – a body now called the European Data Protection Board ("EDPB") – issued guidelines ("EDPB Guidelines") on the setting of administrative fines.[2]

The purpose of this article is to consider the criteria for setting administrative fines under Article 83 of the GDPR in light of the EDPB Guidelines, case law of the CJEU and national courts. Where applicable, we will compare the criteria in Article 83(2) of the GDPR with those used in setting administrative fines for competition law violations, as well as with the methodology used by authorities in the United States for setting fines. We will also consider procedural safeguards under Article 6 of the European Convention on Human Rights.

Pursuant to the EDPB Guidelines, supervisory authorities must consider the proportionality of the corrective measures mentioned in Article 58(2) of the GDPR, including a warning or reprimand, before imposing a fine. When supervisory authorities conclude that an administrative fine is necessary, we propose that they refer to a scoring system that would provide a common framework for calculating the amount of the fine. The scoring system would be based on the number of persons affected by the violation, and would include various multipliers designed to reflect the nature, gravity and duration of the infringement. The score would then be adjusted by the mitigating or aggravating factors listed in Article 83(2) of the GDPR.

Supervisory authorities would remain free to adjust, or in some cases disregard, the scoring system to account for the facts of each case. Yet, a common

[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, O.J.L. 119, 4.5.2016, p. 1–88, *hereinafter* "*GDPR*".

[2] Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, WP 253, 3 October 2017, *hereinafter* "*EDPB Guidelines*".

framework for calculating fines would contribute to transparency, consistency and legal certainty.

1. The principle of equivalence

The first principle mentioned in the EDPB Guidelines is that sanctions should be "equivalent". The principle of equivalence flows from Article 57(1)(g) of the GDPR, which requires that supervisory authorities cooperate "with a view to ensuring the consistency of application and enforcement of this Regulation". Recitals 10 and 11 of the GDPR also stress the need for equivalent sanctions. According to the EDPB, equivalence requires that different supervisory authorities in the EU apply similar fines to similar cases. The principle of equivalence can also be found in the case law of the European Court of Justice, even though its meaning is not exactly the same as that mentioned by the EDPB. In CJEU case law on sanctions, the concept of equivalence means that Member States must apply sanctions to violations of EU law that are equivalent to sanctions applicable to comparable violations of national law.[3]

The GDPR's mechanisms on cooperation and consistency[4] ensure that supervisory authorities coordinate their actions, particularly for violations involving cross-border processing. Article 70(k) of the GDPR empowers the EDPB to create guidelines on corrective measures and administrative fines in order to ensure consistency. In its Guidelines, the EDPB points to its dispute resolution powers under Article 65 of the GDPR as a way for the EDPB to help ensure consistency in fining practices. However, the EDPB's dispute-resolution role would come into play only when one supervisory authority objects to another's proposed sanction, and that would only occur for sanctions that fall under the coordination and consistency mechanism for cross-border processing.

Finally, equivalence requires that a supervisory authority apply the same level of sanctions to the same kind of violation, i.e. non-discrimination in the application of sanctions. The non-discrimination obligation is part of the constitutional obligation of predictability and legality of sanctions.

2. "Effective, proportionate and dissuasive" sanctions

Article 83 states that administrative fines under the GDPR should be "effective, proportionate and dissuasive". These criteria appear explicitly in a number of other EU directives and regulations.[5] The concepts "effective, proportionate and dissuasive" flow from Article 4(3) of the TEU, which requires that Member States take all measures necessary to guarantee the application and effectiveness of Union law. Thus, even if the words "effective, proportionate and dissuasive" were not expressly mentioned in Article 83 of the GDPR, the concepts would nevertheless apply to administrative fines under the GDPR.[6]

Effectiveness, proportionality and dissuasiveness have been defined by CJEU case law. "Effectiveness" means that national law should not render the enforcement of EU law virtually impossible.[7] Effectiveness also includes the principle of equivalence and non-discrimination as regards comparable violations of national law.[8] "Proportionality" means that sanctions should not exceed what is appropriate and necessary to attain the objective legitimately sought by the legislation,

[3] CJEU, Rewe-Zentralfinanz eG v. Landwirtschaftskammer für das Saarland, Case C-33/76, E.C.R. 1976 -01989, 16 December 1976, point 5.

[4] GDPR chapter VII.

[5] *See, e.g.,* Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, O.J.L. 303, 28.11.2018, p. 59–68, art. 5(4),; Regulation (EU) 995/2010 of the European Parliament and of the Council of 20 October 2010 laying down obligations of operators who place timber and timber products on the market; Directive 2008/99/EC of 19 November 2008 on the protection of the environment through criminal law, O.J.L. 295, 12.11.2010, p. 23–34; Directive 2009/123/EC of 21 October 2009 amending Directive 2005/35/EC on ship-source pollution and on the introduction of penalties for infringement, O.J.L.280, 27.10.2009, p. 52–55; Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS), O.J. L. 302, 17.11.2009, p. 32–96.

[6] CJEU, Commission of the European Communities v Hellenic Republic, Case C-68/88, E.C.R. 1989 -02965, 21 September 1989, at 24.

[7] CJEU, Comet BV v Produktschap voor Siergewassen, Case C-45/76, E.C.R. 1976 -02043, 16 December 1976, at 16.

[8] *Id.*

and that when there is a choice between several appropriate measures, recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued.[9] The obligation to consider all appropriate measures and choose the least onerous is also reflected in the EDPB's Guidance: Supervisory authorities "**must** include consideration of all the corrective measures, which would include consideration of the imposition of the appropriate administrative fine, either accompanying a corrective measure under Article 58(2) or on its own".[10] "Dissuasiveness" means that the application of the penalty must result in the party having violated the law being substantially worse off than would be the case if he complied with the law. This requires, at a minimum, that the penalty be sufficiently high so that the guilty party loses any benefit that arose because of its illegal behaviour.[11] Dissuasiveness also requires that one take into effect the likelihood of enforcement:

> 89. A penalty is *dissuasive* where it prevents an individual from infringing the objectives pursued and rules laid down by Community law. What is decisive in this regard is not only the nature and level of the penalty but also the likelihood of its being imposed. Anyone who commits an infringement must fear that the penalty will in fact be imposed on him. There is an overlap here between the criterion of dissuasiveness and that of effectiveness.[12]

The European Competition Authorities Working Group on Sanctions confirms this approach to deterrence: "In order to achieve an adequate level of deterrence, the level of fines should exceed any potential gains that may be expected from the infringement".[13] When discussing the concept of "effective, proportionate and dissuasive" fines, the EDPB Guidelines do not cite any of the CJEU case law referred to above. The EDPB states simply that "[a] more precise determination of effectiveness, proportionality or dissuasiveness will be generated by emerging practice within supervisory authorities (on data protection, as well as lessons learned from other regulatory sectors) as well as case-law when interpreting these principles".[14]

3. The "nature, gravity and duration" of the infringement

Article 83(2)(a) of the GDPR requires that administrative fines take account of the "nature, gravity and duration" of the infringement. As pointed out by the EDPB Guidelines, the GDPR already creates two categories of infringement: those attracting the lower maximum fine (€10 million/ 2% global turnover), and those attracting the higher maximum fine (€20 million/ 4% global turnover). These two levels of maximum fines correspond to violations of different provisions of the GDPR. The lower maximum fines correspond to violations of security obligations and record-keeping obligations, among others. The higher maximum fines correspond to violations of articles going to the heart of the GDPR's substantive obligations, such as the obligation to have a legal basis for processing, or to inform data subjects about processing. By setting different maximum fines, the GDPR signals that violations of the second series of articles are more serious than violating the first series of articles. Thus Article 83 already provides an initial classification of violations according to their nature and gravity: the violations mentioned in Article 83(5) GDPR, which correspond to the highest potential fines (4% global turnover), have a "nature and gravity" score potentially twice as high as the violations mentioned in Article 83(4), which correspond to the lower maximum fines (2% global turnover).

A logical conclusion would be that fines for the violations mentioned in Article 83(5) should generally be twice as high as fines for the violations mentioned in Article 83(4). However, this rule of

[9] CJEU, Ute Reindle v. Bezirkshauptmannschaft Innsbruck, C-443/13, 13 November 2014, at 39.
[10] EDPB Guidelines at p. 7 (bold in the original text).
[11] CJEU, LCL Le Crédit Lyonnais v. Fesih Kalhan, Case C-565/12, 27 March 2014, at 51.
[12] Opinion of Advocate General Kokott, Berlusconi and Others, Joined Cases C-387/02, C-391/02 and C-403/02, 14 October 2004, at 89 (footnotes omitted).
[13] European Competition Authorities (ECA) Working Group on Sanctions, Pecuniary sanctions imposed on undertakings for infringements of antitrust law, Principles for convergence, May 2008, at 3.
[14] EDPB Guidelines at p. 6.

thumb would in many cases conflict with other rules of Article 83, including the rule of proportionality or the rule that fines should take account of the level of damage suffered by data subjects. For example, violations relating to data security obligations are listed in Article 83(4) and therefore benefit from a relatively low score for "nature and gravity". Yet data security violations can create extremely high damages for data subjects; they are among the gravest form of GDPR violations in terms of adverse consequences for data subjects and society. By contrast, a failure to include the duration of data retention in an information notice will in itself cause little or no damage to data subjects and can be considered a form of technical violation. Yet failure to mention the duration of data retention corresponds to a violation of Article 13 that falls under Article 83(5), and therefore attracts a higher "nature and gravity" score than a massive data security breach.

Consequently, the classification between different kinds of violations in Article 83(4) and 83(5) does not provide a reliable benchmark for assessing "nature and gravity". A more reliable proxy for gravity would be the number of data subjects affected, multiplied by the level of damage suffered by each data subject. A violation involving sensitive data, or resulting in identity theft, might correspond to a high damage score for each individual than a violation creating no damage, for example a failure to mention the duration of data retention in an information notice. The level of gravity could therefore be measured by multiplying the number of affected data subjects by an individual damage score. For example, in the case of a data breach involving the loss of sensitive data for 100,000 data subjects, the number of data subjects may be multiplied by a high individual damage score, for example 3. This would yield a nature and gravity score of 100,000 * 3 = 300,000.

Evoking the level of damage suffered by data subjects is always difficult because many data protection violations correspond to harms that are not easy to measure in economic terms. Recital 75 GDPR lists the many forms of the harms that can result from data protection violations, and while it is difficult to put a price tag on many of the harms mentioned in Recital 75, it is possible to create categories of harm, for example, light, medium and severe. This sort of classification is required in any event for data protection impact assessments, where the adequacy of protective measures will depend on the risk of harm. The risk of harm must necessarily take into account the level of impact on each data subject.

Article 83(2)(a) states that in addition to taking into account the number of data subjects affected and the level of damage suffered by them, supervisory authorities should also consider "*the nature, scope or purpose of the processing concerned*". A purpose for data processing with a high level of utility for society, e.g. medical research, might warrant a lower multiplier than a purpose with lower societal benefits, e.g. commercial advertising. In the context of our example, let us imagine that the processing of sensitive data was done for the purpose of creating commercial profiles for advertising. This would generate a high purpose multiplier, for example 3, compared to processing for medical research, which would generate a low purpose multiplier of 1. Thus in the foregoing example, the nature and gravity score would again be multiplied by 3: 300,000 * 3 = 900,000.

In addition to the nature and gravity, the duration of the violation must also be taken into account. Adding duration to the formula is straightforward: It would be sufficient to add a multiplier to the equation corresponding to the number of months during which the violation occurred. In the above example, if the data vulnerability resulting in the loss of sensitive data lasted for 6 months, the resulting nature and gravity score (900,000) would be multiplied by 6, the number of months during which the violation occurred. A linear duration multiplier is routinely used in setting of competition law fines.

The EDPB Guidelines do not suggest using a simple duration multiplier. Instead, the EDPB says that the duration will be an indication of:

a) wilful conduct on the data controller's part, or

b) failure to take appropriate preventive measures, or

c) inability to put in place the required technical and organisational measures.[15]

As our example above shows, creating a consistent methodology for scoring nature, gravity and duration is relatively straightforward. More difficult will be transforming the score into a monetary penalty. Should each point in the score correspond to an administrative fine of 0.20€, 0.50€, 1€, or 2€? We will return to this question in section 6 below.

4. "Minor" infringements

Recital 148 of the GDPR refers to the concept of "minor infringements", which the EDPB explains may be infringements that in the particular circumstances do not pose a significant risk to the rights of data subjects, and do not affect the essence of the obligation in question. For minor infringements, Recital 148 states that a "reprimand may be sufficient". This corresponds to the requirement, mentioned in section 2 above, that supervisory authorities systematically consider application of all alternative remedies in Article 58, and choose the one that is most proportionate in the circumstances. A failure to mention the duration for the retention of data in the information notice may be an example of a minor infringement, particularly if the actual retention periods for data used by the data controller are not excessive. By contrast, a failure to mention the duration of data retention combined with excessively long data retention periods would likely be viewed as affecting the "essence of the obligation in question". The violation would in that case not be a minor infringement for purposes of Recital 148.

5. Other factors

Article 83(2) lists ten other factors that supervisory authorities must take into account when setting fines. These factors resemble the aggravating and mitigating factors set forth in the European Commission guidelines on setting fines for competition law violations[16], as well as in the United States Sentencing Guidelines[17].

A. The intentional or negligent character of the infringement

The EDPB Guidelines state that intentional violations, "demonstrating contempt for the provisions of the law, are more severe than unintentional ones and therefore may be more likely to warrant the application of an administrative fine."[18] The Guidelines give several examples of intentional violations, citing for example "unlawful processing authorised explicitly by the top management hierarchy of the controller, or in spite of advice from the data protection officer or in disregard for existing policies". The involvement of senior management is an aggravating factor under the United States Sentencing Guidelines as well.[19] According to the EDPB, "failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them) may be indicative of negligence."[20]

The EDPB refers to "grey areas" where more extensive investigations will be needed to determine whether a violation is intentional or negligent. The EDPB Guidelines do not discuss infringements that result from good faith interpretations of the GDPR by the data controller that diverge from the interpretation of the supervisory authority. The GDPR puts the responsibility on the data controller to interpret many of the general obligations contained in the GDPR, and to demonstrate the data controller's compliance with those obligations. For example, it is up to the data controller to design the presentation of information to data subjects in a "concise, transparent, intelligible and easily accessible form, using clear and plain language"[21]. The supervisory authority may disagree with the

[15] EDPB Guidelines at p. 11.
[16] [EC] Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No 1/2003, (2006/C 210/02), OJ C 210, 1.9.2006, p. 2–5, 1 September 2006.
[17] United States Sentencing Commission, Guidelines Manual, ch. 8 (*Sentencing of Organizations*), 1 November 2018, *hereinafter USSC*, p. 509.
[18] EDPB Guidelines at p. 12.
[19] USSC, *supra* note 17, at p. 529, §8C2.5(b).
[20] EDPB Guidelines at p. 12.
[21] GDPR art. 12.

data controller's choices, and find that the data controller's approach is not as transparent and accessible as the supervisory authority would like. This difference in interpretation could constitute a violation. But would such a violation be intentional, negligent, or neither? The same question would arise where a supervisory authority does not agree with the risk analysis and mitigation measures chosen by the data controller in its data protection impact assessment, or where the supervisory authority does not agree with the balancing done by the data controller in connection with "legitimate interest" processing. The GDPR emphasizes risk-based decision-making by the data controller based on the data controller's own interpretation of the GDPR's provisions. In some cases, the supervisory authority will not agree with the data controller's approach. Indeed, it would be surprising if the supervisory authority *did* agree, unless the data controller simply copied an approach previously approved by the supervisory authority. In many cases, the supervisory authority will evaluate the data controller's choices after an incident has occurred or a complaint has been made, leading to a normal bias that the data controller's measures were not sufficient.

Regrettably, the EDPB Guidelines do not discuss cases where the data controller has made a good faith effort to interpret the GDPR's obligations in the spirit of accountability, but it turns out that the supervisory authority disagrees with the data controller's approach. Such a case should be a "non-negligent" infringement of the kind mentioned by the EDPB in connection with Article 83(2)(c). For these situations, only a warning or reprimand under Article 58 GDPR would be appropriate, deterrence not being necessary for a good faith mistake.

B. Any action taken by the controller or processor to mitigate the damage suffered by data subjects

According to the EDPB Guidelines, quick and responsible action by the data controller to mitigate the consequences of a violation should be taken into account as a mitigating factor:

This provision acts as an assessment of the degree of responsibility of the controller after the infringement has occurred. It may cover cases where the controller/processor has clearly not taken a reckless/negligent approach but where they have done all they can to correct their actions when they became aware of the infringement.[22]

The EDPB recognizes the existence of "non-negligent" infringements in this context, i.e. a situation where the data controller has not taken a reckless or negligent approach and done all it could to correct the situation. According to the EDPB, this situation may tip the balance away from imposition of a fine, toward other more proportionate corrective measures, such as a warning, under Article 58 GDPR. It is a pity that the EDPB did not examine the case of "non-negligent" infringements when discussing Article 83(2)(b) of the GDPR, which relates to the intentional or negligent character of the infringement.

C. The degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

As pointed out by the EDPB in its Guidelines, Articles 25 and 32 of the GDPR impose on data controllers an obligation of means, rather than an obligation of a given outcome. The controller "must make the necessary assessments and reach the appropriate conclusions" on what constitutes appropriate means to ensure compliance with the GDPR.[23] This will depend in part whether the data controller has implemented sufficient technical and organisational measures, and involved the appropriate level of management in the organisation. Assessing the level of responsibility of the data controller boils down to determining whether the data controller has an effective GDPR compliance program in place. This mitigating factor for GDPR financial penalties is directly inspired by the United States Sentencing Guidelines, which permit organisations to earn positive points in sanction

[22] EDPB Guidelines at pp. 12-13.

[23] EDPB Guidelines at p. 13.

proceedings, if they can show that they have an effective compliance program in place.[24]

D. Any relevant previous infringements by the controller or processor

Recidivism is an aggravating factor for sanctions under the GDPR. This principle is also applied in the European Commission's guidelines on competition law fines[25], and the United States Sentencing Guidelines[26].

E. The degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

The EDPB Guidelines provide little useful guidance on how the cooperation factor should be applied, other than to point out that cooperation which is required anyway under law should not be considered a mitigating factor. The EDPB points out that if an organisation responded "in a particular manner" during the investigation phase and the organisation's cooperation reduced the impact of the violation, this may be a mitigation factor.

Cooperation is a well-known mitigation factor both in EU competition cases and in United States investigations. For competition law cases, companies earn mitigation credit if they "effectively cooperated with the Commission outside the scope of the Leniency Notice and beyond its legal obligation to do so".[27] Companies also can benefit from mitigating circumstances if they "terminated the infringement as soon as the Commission intervened".[28]

Under the United States Sentencing Guidelines, cooperation is a major factor for reducing fines, which is why companies generally prefer to cooperate with the United States authorities in major investigations. To earn cooperation credit, companies in the United States must actively help the authorities determine the facts surrounding the potential violation and identify relevant individuals:

> In order for a company to receive any consideration for cooperation under this section, the company must identify all individuals substantially involved in or responsible for the misconduct at issue, regardless of their position, status or seniority, and provide to the Department all relevant facts relating to that misconduct.[29]

Under both EU competition law, and the United States Sentencing Guidelines, refusal to cooperate, or obstruction of justice, can be an aggravating factor.

F. The categories of personal data affected by the infringement

The EDPB Guidelines point to the nature of the personal data, as well as whether the data were encrypted. Presumably unencrypted sensitive data would point to a more serious violation, meriting a higher fine, than encrypted non-sensitive data. As mentioned in section 3 above, the nature of the data involved will have already been taken into account when determining the "nature and gravity" of the infringement. We suggested a specific multiplier that would reflect the damage associated with different kinds of data.

G. The manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement

Article 33 of the GDPR imposes on data controllers an obligation to notify the supervisory authority about personal data breaches without undue delay. As a consequence, the EDPB Guidelines provide that the notification of a personal data breach to the supervisory authority is not a mitigating factor as it

[24] USSC, *supra* note 17, at p. 517, §8B2.1.
[25] [EC] Guidelines on the method of setting fines, *supra* note 16, at 28.
[26] USSC, *supra* note 17, at p. 530, §8C2.5(c).
[27] [EC] Guidelines on the method of setting fines, *supra* note 16, at 29.
[28] *Id.*
[29] United States Department of Justice [USDJ], Justice Manual, 9-28.000 (Principles of Federal Prosecution Of Business Organizations), 9-28.700 (The Value of Cooperation).

corresponds to the mere fulfilment of the obligation set by abovementioned Article 33.

By contrast, a failure to notify or a failure to adequately assess the extent of the data breach resulting in an insufficient notification which does not meet the requirements set by Article 33 of the GDPR is an aggravating factor. According to the EDPB, data controllers may thus "be considered by the supervisory authority to merit a more serious penalty i.e. it is unlikely to be classified as a minor infringement"[30], as mentioned in section 4 above.

H. Where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures

In order to assess this criterion, the EDPB recommends that supervisory authorities take into account their previous contacts with data controllers or processors, when monitoring compliance with previous corrective measures. The EDPB points out that, as opposed to the recidivism aggravating factor, this criterion aims at reminding supervisory authorities to refer to previously imposed measures with regard to the same subject matter.

I. Adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

According to the GDPR, adherence to approved codes of conduct or approved certification mechanisms may be used by the controller to demonstrate compliance with its obligations.

In case of a personal data breach, the EDPB points out that "adherence to an approved code of conduct might be indicative of how comprehensive the need is to intervene with an effective, proportionate, dissuasive administrative fine or other corrective measure from the supervisory authority".[31] Yet, the EDPB also indicates that supervisory authorities might consider that the self-regulatory measures taken by the body in charge of administering the code "are effective, proportionate or dissuasive enough in that particular case without the need for imposing additional measures from the supervisory authority itself".

Articles 41(1) and 43(1) of the GDPR provide that the powers of the monitoring body are "without prejudice to the tasks and powers of the competent supervisory authority". The EDPB Guidelines point out that the supervisory authority is not under an obligation to take into account sanctions previously imposed by the monitoring body.

Last, the EDPB indicates that adherence to approved codes of conduct or approved certification mechanisms can be used to assess the intentional or negligent character of the infringement mentioned in section 5.1 above.

J. 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

The EDPB Guidelines provide little guidance as to the use of other aggravating or mitigating factors. The EDPB only points out that profit obtained as a result of the infringement should be compensated through measures which have a "pecuniary component", and "may constitute a strong indication that a fine should be imposed".[32]

6. Lessons from competition law

The GDPR's system for administrative fines is in many respects similar to the system used in European competition law. Both systems have maximum fines based on the global turnover of the organisation. Both systems take into account the gravity and duration of the violation as well as the level of cooperation with authorities. In competition law, the European Commission and national competition authorities have developed a methodology to help contribute to legal certainty[33]

[30] EDPB Guidelines at p. 15
[31] EDPB Guidelines at p. 15
[32] EDPB Guidelines at p. 16

[33] CJEU, Groupe Danone v Commission of the European Communities, Case C-3/06 P, E.C.R. 2007 I-01331, 8 February 2007, at 23.

and transparency[34]. Within this methodology, authorities are then free to take special factors into account, but the objective of the methodology is to give authorities a consistent starting point.

Under the European Commission's 2006 competition law guidelines the starting point for calculating administrative fines is the turnover of the relevant companies relating to the violation. For example if the violation relates to a cartel in the sale of steel in France, the starting point for calculation of the fine will be the amount of the undertaking's annual sales of steel in France in the market in which the violation occurred. A percentage is then applied to that starting amount, which the Commission suggests should be 30%. 30% is a rough approximation of the gross profit realised by the company from the sales.

According to the Commission, taking a percentage of the gross sales resulting from the incriminated behaviour is a good starting point for measuring the gravity of the violation. To measure the duration of the violation, the Commission measures the number of years during which the violation occurred. For example in the case of a cartel relating to the sale of steel products in France, if the annual gross sales are €100 million, the baseline annual amount would be equal to 30% x €100 million or €30 million. If the cartel lasted six years, this baseline amount of €30 million would be multiplied by 6, yielding €180 million. This would be the starting amount of the fine, which would then be subject to a series of aggravating or mitigating adjustments. Here, the methodology is similar to what we see in Article 83 of the GDPR.

Once the aggravating and mitigating factors have been applied to the original baseline amount, the Commission's methodology for competition law then requires verification that the resulting amount does not exceed the statutory cap of 10% of the global revenues of the relevant undertaking.

Much of the methodology used in setting competition law fines can be applied to GDPR violations with the exception of the first step, which consists of setting the baseline amount for the fine. In competition law cases there is a market of relevant products or services in which the competition law violation occurred. The reason the anticompetitive behaviour occurred in the first place was to increase the company's sales and/or margins in that relevant market. Consequently the level of sales into that market can serve as a good proxy for measuring the importance of the infringement and its impact on the economy. For data protection violations, the process is more difficult because the violations do not relate directly to higher prices, higher market shares or higher margins for the companies involved.

Data protection violations are not supposed to translate necessarily into economic damage for data subjects. Article 83 of the GDPR mentions the level of damage suffered by data subjects as one factor to be taken into account, but given the human rights approach taken under the GDPR, it seems difficult to use the level of damage suffered by data subjects as a starting point for a calculation of administrative fines. Indeed, data protection authorities are loath to translate data protection violations into measurable economic harm. And yet to achieve consistency and predictability in setting of administrative fines under the GDPR, there needs to be some method for calculating the initial amount of the fine, which is then subject to adjustment based on aggravating and mitigating factors. Otherwise the diverse approaches to fine determination under the GDPR will lack consistency and legal certainty.

The most obvious starting point for setting a fine would be the calculation of the number of data subjects affected by the relevant violation. The number of persons affected would be one factor indicating the gravity of the violation: a violation affecting 3 million people is usually more serious, than a violation affecting 3 people. A second factor would be the type of data involved in the violation. For example routine commercial data might warrant a low multiplying factor of one, whereas sensitive personal data might warrant a multiplier of three.

[34] Autorité de la concurrence [French Competition Authority], Notice of 16 May 2011 on the Method Relating to the Setting of Financial Penalties, at 14.

The duration of the infringement is also easy to calculate. The same methodology could be used as the one used in competition law, i.e. the baseline score is multiplied by the number of years during which the violation took place.

As we demonstrated in Section 3, it would be relatively straightforward to develop a scoring system. The real challenge lies in transforming a score into a monetary amount. Should a "point" in the scoring system translate into 0.20€, 0.50€, 1€ or 100€? As noted previously, data protection authorities are loath to put a price on individual data protections violations. Yet setting a monetary amount is required for administrative fines, and there must be a consistent approach.

The European Court of Justice has defined the concept of dissuasive penalties as penalties that are sufficient to ensure that the illegal conduct is not profitable. Corporations typically pursue anticompetitive activities in order to increase their sales and/or margins. This also holds true for data protection violations. A data protection violation may occur because a company wants to minimize its costs or increase its revenues compared to the situation in which it does not violate data protection requirements. Comparing the profits of a company in the situation where it complies scrupulously with data protection requirements to the situation in which it does not comply would provide a good picture of illegally gained profits of the company, and those profits could be the starting point for any discussion of administrative fines. Profits are expressly mentioned in Article 83(2)(k) of the GDPR, but they are cited as an aggravating or mitigating factor, not as the starting point for calculating GDPR fines.

Determining profits may also be too complex a criterion for regulatory authorities in practice. In many cases, profits will be non-existent, or will be too dependent on confidential information held by the relevant company. Therefore, it may make sense, as in competition law, to create a simplifying rule. The simplifying rule would be the number of data subjects affected, multiplied by the factors mentioned in Section 3 above. This would yield an initial fine amount that could then be increased, or decreased, by the supervisory authority based on all the factors mentioned in Article 83(2) of the GDPR.

It is hard to think of any starting point for fines other than the number of data subjects affected by the violation. The difficulty will be setting an initial monetary amount to correspond to each point in the score. This will necessarily force data protection authorities to translate data protection harm into an economic unit. The scoring systems, and the economic unit, would then serve as the starting point when developing a sanction approach in a given case.

The scoring system would come into play only in cases where the supervisory authority determines, after examining the proportionality of all the other corrective measures in Article 58 of the GDPR, that an administrative fine is necessary.

7. Appropriate procedural safeguards

The GDPR provides that the exercise of the sanctioning powers conferred on the supervisory authorities shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection and due process.[35] This is in line with French case law on independent administrative authorities, and in particular the Restricted Committee of the CNIL.

In a decision dated 30 December 1982, the French Constitutional Council ruled, with respect to tax law, that constitutional principles applicable in punitive matters[36] shall apply to any sanction having the character of a punishment, even when such sanction is imposed by a non-judicial authority.[37] The French Supreme Court ruled that Article 6§1 of the

[35] *See* GDPR recital 148, arts. 58(4) and 83(8).

[36] Notably, the principle according to which "[t]he Law must prescribe only the punishments that are strictly and evidently necessary; and no one may be punished except by virtue of a Law drawn up and promulgated before the offense is committed, and legally applied", French Declaration of Human and Civic Rights, 26 August 1789, art.8.

[37] Conseil constitutionnel [French Constitutional Council], no. 82-155 DC, 30 December 1982.

European Convention on Human Rights (right to a fair trial) is applicable to independent administrative authorities which are invested with the power to issue financial sanctions.[38]

For the first time in 1999, the French Administrative Supreme Court (*Conseil d'Etat*) decided that when issuing financial sanctions, the Financial Market Authority must be considered as determining "criminal charges" within the meaning of Article 6§1 of the European Convention on Human Rights.[39] Accordingly, this independent administrative authority is obliged to comply with the rights set forth in the Convention. By contrast, on the same day, the French Administrative Supreme Court ruled that a CNIL deliberation is not handed down by a "tribunal" within the meaning of Article 6(1) of the European Convention on Human Rights.[40] In a decision dated 19 February 2008, the French Administrative Supreme Court reversed its case law and ruled that the CNIL can be considered a "tribunal" within the meaning of Article 6§1 of the European Convention on Human Rights.[41] The French Constitutional Council recalled in 2009 that the sanctioning power vested in the independent administrative authorities must be accompanied by measures intended to ensure protection of constitutional rights and liberties.[42]

In 2014, the French Administrative Supreme Court decided that the Restricted Committee of the CNIL, when exercising its sanctioning powers, must be considered a "tribunal" within the meaning of Article 6§1 of the European Convention on Human Rights and, as a consequence, must comply with the procedural requirements set by the European Convention on Human Rights when imposing sanctions, notably the independence and impartiality requirements.[43] The French Supreme Court specified that the requirements of Article 6§1 of the European Convention on Human Rights apply to the sanction procedure, and not to the preliminary phase of inspections conducted by the staff of the CNIL.[44]

In light of the above, the Restricted Committee, when exercising its sanctioning powers as a "tribunal", must comply with the general principles derived from European law (notably requirements of Article 6§1 of the European Convention on Human Rights), as well as the French constitutional principles applicable to criminal sanctions. In theory, the following rights and principles will act as safeguards to protect the alleged offenders' rights. In practice, many aspects could be improved.

According to a long line of case law of the European Court of Human Rights, legal persons can benefit from the right to a fair trial set forth by Article 6 of the European Convention on Human Rights. It provides, among other things, the right for any person being accused to be informed in a language "which he understands" of the nature of the accusations against it. In a recent case, the European Court of Human Rights considered that a notification of accusations in a foreign language against a person who had only a limited knowledge of this language constituted "a violation of his right to a fair trial".[45] In addition, the right to a fair trial involves the right for the person "to have adequate time and facilities for the preparation of his defense".[46] Despite the fact that abovementioned Article 6 applies to sanction proceedings before the Restricted Committee of the CNIL, the current procedural rules do not require a translation or an extension of delay for foreign undertakings or entities to prepare their defence.

Under constitutional principles of proportionality and due process, the alleged offender must be informed with clarity and precision of the exact violations it has been accused of committing. Accusations should not be too general and all-

[38] *E.g.* for the French Securities Exchange Commission: Cour de cassation [Cass.][French supreme court for judicial matters], no. 97-16440, 5 February 1999.
[39] Conseil d'Etat, [French Administrative Supreme Court], no. 207434, 3 December 1999.
[40] Conseil d'Etat, [French Administrative Supreme Court], nos. 197060 and 197061, 3 December 1999.
[41] Conseil d'Etat [French Administrative Supreme Court], no. 311974, 19 February 2008.
[42] Conseil constitutionnel [French Constitutional Council], no. 2009-580 DC, 10 June 2009.
[43] Conseil d'Etat, [French Administrative Supreme Court], no. 353193, 12 March 2014.
[44] Conseil d'Etat, [French Administrative Supreme Court], no. 371196, 18 November 2015.
[45] Vizgirda v. Slovenia, [2018] ECHR 674, 28 August 2018.
[46] The European Convention on Human Rights art. 6(3)(b).

encompassing to permit the offender to defend itself with regard to precise factual allegations. This would violate both the presumption of innocence and the right to a fair trial. In a case brought before the Court of Justice of the European Communities, the reasons given by the European Commission in its decision sanctioning anticompetitive agreements were too general to enable the appellant to defend the case and challenge the assessment. The Court ruled that:

> It is settled case-law that in all proceedings in which sanctions, especially fines or penalty payments, may be imposed, observance of the rights of the defence is a fundamental principle of Community law which must be complied with even if the proceedings in question are administrative proceedings […]. To that end, Regulation No 17 provides that the parties are to receive a statement of objections which must set forth clearly all the essential facts upon which the Commission is relying at that stage of the procedure. That statement of objections constitutes the procedural safeguard applying the fundamental principle of Community law which requires observance of the rights of defence in all proceedings […]. That principle requires, in particular, that the statement of objections which the Commission sends to an undertaking on which it envisages imposing a penalty for an infringement of the competition rules contain the essential elements used against it, such as the facts, the characterisation of those facts and the evidence on which the Commission relies, so that the undertaking may submit its arguments effectively in the administrative procedure brought against it.[47]

Hence, the Restricted Committee must observe the rights of defence and the accusations must be specified in sufficient detail to permit an effective defense. As to the amount of the fine, the Report should provide information justifying the amount to ensure a fair opportunity to respond for the alleged offender, and administrative fines should not exceed what is necessary to effectively sanction the offenders and deter data protection violations.

The French Administrative Supreme Court recently applied the principle of proportionality to a decision of the Restricted Committee of the CNIL, which imposed on an undertaking an administrative fine of €50,000 and the publication of the sanction decision on two websites for an unlimited period of time.[48] The Court ruled, on the one hand, that the administrative fine was proportionate having taken into account the nature, gravity and duration of the breaches, and, on the other hand, that the complementary sanction (i.e. the unlimited publication) was excessive. The Court thus set a two-year publication period.

In the same decision, the Court applied Article 7 of the European Convention on Human Rights which sets forth the principle that only the law can define a crime and prescribe a penalty (no punishment without law). The Court ruled that the Restricted Committee complied with aforementioned Article 7 because Articles 34 and 35 of the former French Data Protection Act precisely defined the obligations of the data controller on the one hand, and that the formal notice issued by the CNIL characterized in a clear and precise way the breaches identified against the offender and the suggested remedies. This decision illustrates the application by the French Administrative Supreme Court of Articles 6 and 7 of the European Convention on Human Rights to the sanction decisions handed down by the Restricted Committee of the CNIL.

Another procedural safeguard is the right to an effective judicial remedy set forth by Article 78 of the GDPR. In this respect, the decision of the Restricted Committee can be appealed before the French Administrative Supreme Court within a 2-month delay (4 months for companies located abroad).

[47] ECJ, Papierfabrik August Koehler AG, Bolloré SA, Distribuidora Vizcaína de Papeles SL v Commission of the European Communities, (Joined Cases C-322/07 P, C-327/07 P and C-338/07 P), O.J.C 256, 24.10.2009, p. 3–3, 3 September 2009, at 34-36 (references omitted).

[48] Conseil d'Etat, [French Administrative Supreme Court], no. 396050, 19 June 2017.

Conclusion

The principles of "effective, proportionate and dissuasive" sanctions have been interpreted by the CJEU, and those interpretations will naturally apply to sanctions imposed under the GDPR. The principle of proportionality, in particular, requires that supervisory authorities consider the full range of corrective measures and choose the one that is the least intrusive while still permitting the attainment of the objectives of the GDPR. In many cases, a warning or reprimand will be sufficient.

When a fine is considered necessary, we suggest that the EDPB develop a methodology for calculating the amount of the fine, based on a point system. This approach has been used for competition law sanctions, and increases transparency, consistency and legal certainty of sanctions. A major difficulty in the context of GDPR will be translating the point system into economic units corresponding to fines. Competition law violations can be measured in economic terms. Data protection violations are more difficult to measure economically. Therefore, the competition law approach cannot be transposed as it is to the GDPR. Given the human rights focus of the GDPR, data protection authorities are not accustomed to attributing economic values to data protection violations. Yet, translating violations into monetary amount is inevitable when setting administrative fines, so supervisory authorities will need to find a common method for doing so, particularly because fines are likely to become larger under the GDPR.

The scoring system we suggest in this article is first based on the number of data subjects affected by the violation. A violation affecting 3 people would have a lower score than a violation affecting 3 million. Various multipliers would then be applied to this initial score, to reflect the seriousness of the violation, the kind of data involved, the purpose of the processing, and the duration of the infringement. Once an adjusted score is obtained, supervisory authorities would then apply the aggravating and mitigating factors listed in Article 83(2) of the GDPR. In appropriate cases, supervisory authorities could decide to modify the point system, or even disregard it entirely, to reflect the particular circumstances of the case. However, without a common scoring system, setting administrative fines will be based on intuitive and subjective factors that will undermine the GDPR's objectives of consistency and predictability.