EasyChair Preprint

№ 582

Fines under the GDPR

Paul Nemitz

October 21, 2018

Fines under the GDPR

Introduction and Outline

The introduction of substantial fines for infringements in Article 83 GDPR constitutes an important development of European data protection law. This article discusses the innovation in comparison to the previous directive, with a special emphasis on the inspiration the EU rules and practice of fining in Competition law contain for the fining under GDPR. It first sets out thoughts on the purpose of fines and the structure of Article 83 GDPR. Next it demonstrates how competition law is inspiring the fining rules under GDPR and why DPAs are under a general duty to impose fines. It then discusses considerations on the amounts of fines and the special case of Cumulation of infringements as well as the notion of "the undertaking", so important both in competition law and the GDPR. As a reminder of past incoherence rather than as a starting point for future fining practices, the article closes by reviewing the diversity of fines under the previous directive and ends with a call on the Data Protection Board to quickly establish a publicly accessible database on fines imposed by DPAs, in order to create the transparency necessary to ensure a coherent application of the GDPR across the European Union. In the conclusion, this Articles calls on DPAs to learn from Competition law and to acquire the skills necessary for rigorous fining bringing about the necessary deterrent effect.

The purpose of fines and the structure of Article 83 GDPR

Imposing fines will often have a higher disciplinary function than other remedies. Fines serve to discourage further infringements. Art. 83 GDPR serves both special prevention and general prevention, since high fines for misconduct are attracting widespread attention, especially in the case of controllers or processors known in the market and to the general public. They ensure that efforts of compliance are undertaken in addition to pure profitability investments and a fortiori that the economic advantage that controllers or processors derive from infringements of GDPR, if any, do not remain with them (see Art. 83 (2) (k) GDPR).The fines, if high enough, thus can reduce the incentives of non-compliance. In view of the potentially substantial fines, it is to be expected that, under Article 83 GDPR, the fine for the relevant players will provide the greatest, if not the decisive, incentive to act lawfully and thus to respect the rights of the data subject in the processing of their personal data and to make the system of the GDPR as a trust framework for personal data processing work in Europe and beyond.

Against the background of the digital economy, which is steadily increasing in importance, the GDPR thus ensures that the market continues to serve the interests of individuals and the general public. Entrepreneurial for profit activity shall not deprive individuals of their fundamental right to data protection. The market regards any data more and more as a tradable standardised commodity ("data is the new oil", "data is the currency of the future"). The financial burden associated with fines under Article 83 GDPR ensures that the market is encouraged to respect the specific fundamentals rights positions which are inherent in personal data, which legally cannot be treated and traded in Europe like the commodities oil and currency.

Whether Article 83 GDPR can fulfil its function in practice will depend crucially on its implementation by the Data Protection Authorities: It will be essential that the supervisory authorities are adequately resourced in terms of infrastructure, personnel and finances in order to be able to fulfil their role, also vis-à-vis internationally and globally active companies, thus enabling the GDPR to be implemented and applied effectively. The experience of Competition Law shows that most decisions on the imposition of fines are contested in law by the parties concerned up to the last instance. In this respect too, the supervisory authorities should ensure that they are adequately qualified and sufficiently staffed for lengthy legal disputes.

Article 83 GDPR provides for a differentiated and flexible system of fines, which allows and obliges the supervisory authorities to sanction violations of the GDPR with appropriate fines in order to deter future infringements. Paragraph 1 sets the standards for the entire sanction system in the GDPR, to which concrete measures must adhere. Paragraph 2 lays down specific criteria to be taken into account when determining the amount of a fine in a specific case. Paragraph 3 regulates cases of cumulation of data protection infringements and sets the maximum amount of the fine for them. Paragraphs 4 and 5 qualify violations of the provisions of the GDPR depending on their significance in simple or qualified violations, which accordingly result in lower or higher fines. Paragraph 6 provides for a further increase in the fine for violations of prior orders from supervisory authorities. Paragraph 7 contains a limited opening for Member States, which can exempt the public sector from fines to a limited extent. Paragraph 8 clarifies that the fines procedure and the ensuing judicial proceedings must comply with the requirements of the Union and Member State law. Finally, Paragraph 9 contains special rules for Denmark and Estonia whose legal systems do not provide for the power of authorities to impose fines (see recital 151 GDPR).

The inspiration from Competition law for finding under GDPR

Concretisations relating to Art. 83 GDPR can be found in recitals 148, 150, 151, 152 and 153 GDPR. Special attention should be paid, in addition to the fining practice of the Commission and the national authorities on competition law, to the Guidelines of 3 October 2017 of the Article 29 Working Party[1] under Article 70 (1) (k) GDPR. They are intended to ensure the uniform application of Art. 83 GDPR.

These guidelines are for good reasons not so detailed that controllers and processors can insert fines into their economic calculation ex ante as part of an illegal business model. This would allow them to set prices accordingly to cover the risk of the fines calculated in advance and thus deprive the fines of any deterrent effect, contrary to what the regulation provides. The Art. 29 Working Party announces in its Guidelines under Chapter III after footnote 10 in a bracketed sentence that "detailed calculation work would be the focus of a potential subsequent stage of this guideline". It can only be hoped that wisdom guides this work so as to avoid that it is made possible in that way for controllers and processors to calculate fines in advance, which "would devalue their effectiveness as a tool" (see Guidelines II.1. after footnote 6).

[1]Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679, Article 29 Data Protection Working Party, 17 / EN WP 253 of 3 October 2017;

The GDPR in its fining system is inspired by the system of fines in European Competition Law and uses its methodology in large part. In particular, the determination of fines in terms of a percentage of overall turnover and a cap of fines determined by a set percentage of turnover of the undertaking concerned (4% in Article 83 GDPR), is inspired by the same methodology in the Commission Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No 1/2003, which provides in Paragraph 32:

"*The final amount of the fine shall not, in any event, exceed 10 % of the total turnover in the preceding business year of the undertaking or association of undertakings participating in the infringement, as laid down in Article 23(2) of Regulation No 1/2003*."[2]

Also, the Merger Regulation, in Article 14,[3] follows such a methodology of fine calculation based on turnover. A case of its application relevant to data protection, the Facebook/WhatsApp case, is discussed further below.

It is thus not surprising that recital 150 GDPR explicitly refers to Articles 101 and 102 TFEU, the basic provisions in the Treaty on Competition law, for the definition of an undertaking on which a fine is imposed and in relation to which turnover has to be calculated. to be used also in the GDPR for this purpose. In the Guidelines of 3 October 2017, the Art. 29 Working Party in addition refers in footnote 4 to specific ECJ jurisprudence in the area of Competition Law.[4]

Both data protection and competition law fall within the category of special economic administrative law. In these fields of law, infringements are often a matter of cost reducing intention or negligence, motivated by the pursuit of profit. There are costs related to compliance and in some cases high financial incentives for both competition and data protection breaches. In both areas of law, directly or indirectly, natural persons, as consumers and citizens concerned, are the victims of these infringements, either by economic disadvantage or by a deterioration of fundamental rights positions, or both.

The European experience in Competition Law shows that the public enforcement, based on ex-officio actions and complaints, is the main driver of compliance. Private enforcement and actions for damages, even where special legislation for that purpose exists,[5] play a smaller role, with the later often being efficient only as a follow on of public enforcement findings of illegality.[6] A fortiori the private enforcement or damages claims in Data Protection Law have

[2]Guidelines on the method of setting fines according to Art. 23, para. 2, pt. A VO (EC) no. 1/2003, OJ. 2006 C 210, 2;

[3]Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings, OJ. L 24 of 29.1.2004;

[4]Generally on the relationship between privacy and competition law Costa- Calbral, Lynskey, Family Ties: The intersection between Data Protection and Competition in EU Law, in: CMLR 2017, p. 11; on the relationship between data protection law and consumer protection law Helberger, Borgesius, Reyna, The perfect match ? A closer look at the relationship between EU Consumer Law and Data Protection Law, in: CMLR 2017, 1427;

[5]Directive 2014/104 / EU adopting certain provisions on damages actions under national law for infringements of competition regulations of the Member States and the European Union, OJ. 2014 L 349, 1;

[6]See for details "Private Enforcement of Competition Law", Basedow, Terhechte, Tichy (Editors), 2011,

so far in practice played no significant role in Europe. It is likely that as in Competition Law, public enforcement will be the main compliance driver in the area of data protection. The complexity and intransparency of the processing of personal data led the primary legislator in the first place to foresee strong and independent Data Protection Authorities in Art. 16 (2) TFEU and Art. 8 of the Charter of Fundamental Rights. This is also the key argument in favour of strong public enforcement, now that the regulation provides the DPAs the tools for this purpose. In addition, the usual enormous asymmetry of economic power and information between the individual and the controllers and processors in the digital economy is a key argument for strong public enforcement: The individual simply cannot be left alone in this asymmetry. The creation of ever more individual rights has only a small positive compliance effect on controllers and processors if it is not accompanied with strong public enforcement.

This reality must have an impact on the application of Article 83 GDPR in individual cases. In many cases, its interpretation and application will be inspired by similar considerations such as those in competition law, for example in Articles 14 on fines in the Merger Regulation. It provides that the Commission may impose fines not exceeding 1 % of the aggregate turnover of the undertaking or association of undertakings concerned where, intentionally or negligently, they supply incorrect or misleading information in a submission, certification, notification or supplement thereto, in the context of Merger investigations.[7]

This provision was recently applied in a case concerning personal data and data protection questions, namely profiling, in Commission Decision of 18 May 2017 imposing fines under Article 14(1) of Council Regulation (EC) No 139/2004 for the supply by an undertaking of incorrect or misleading information.[8] In this case, the European Commission imposed a fine of 110 Million Euros because despite the availability of automated matching solutions between Facebook and WhatsApp, Facebook had stated in the investigation relating to the Merger of WhatsApp and Facebook that user matching between Facebook and WhatsApp would either have to be done manually by users, and would therefore be insufficient and unreliable; or require Facebook to significantly re-engineer the app's code.

This case is important as it demonstrates the risk – or one might call it the temptation – to lie when it comes to describing facts on processing of personal data to the regulator, maybe in the hope that the regulator will not master the technical complexities involved. It will be important, for gaining the necessary respect and cooperation in the increasingly complex maze of processing of personal data, that DPAs rigorously increase fines at the slightest sign of negligent or intentional misleading statements when it comes to establishing facts relevant for their decisions. At the core of the unconditional duty to cooperate with the DPAs of controllers and processors as well as Data Protection Officers (see Articles 31 and 39 (1) (d) GDPR) is the duty to state the truth and DPAs need to ensure respect of this through a rigorous fining practice following this example set by the European Commission.

The fact that in the initial phase of the interpretation and application of the GDPR comparable rules in competition law will often provide orientation does not rule out that data protection law will later develop into an independent practice. However, this practice should always seek

[7]Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings, OJ. L 24 of 29.1.2004;
[8]Case M.8228 — Facebook/WhatsApp (Art. 14(1) proc.), notified under document number C(2017)3192), see at https://publications.europa.eu/en/publication-detail/-/publication/f0da1066-8d12-11e7-b5c6-01aa75ed71a1/language-en/format-PDFA1A;

coherence of the legal system as a whole, including in the relationship between fines in competition law and in data protection law. In addition, it obviously must pursue consistency between the actions of data protection authorities across all Member States. With the entry into force of the Regulation, data protection authorities must be prepared to sanction infringements of the Regulation as consistently as possible under the Regulation, and in order to obtain a strong deterrent against non-compliance, as competition authorities have done for a long time in competition law infringements.

It would not be in line with the basic legal protection obligation of data protection authorities and the principle of coherence of the legal system if DPAs would leave it to the admittedly for the time being far better-equipped competition authorities and their stringent enforcement tradition to sanctioning of breaches of the GDPR, for example if committed by dominant companies. The investigation and then preliminary assessment of the Federal German Cartel Office, the German competition authority, in the Facebook procedure touched on data protection law and in its preliminary statement of 19.12.2017 came to the conclusion that the collection and exploitation of data from third-party sources outside the Facebook website is abusive.[9] This case and the Commission decision in Facebook/WhatsApp cited above demonstrate the close relationship between competition and data protection enforcement. They open the door to far more intense cooperation and mutual learning between EU Competition authorities (the Commission and Member States' Competition authorities) and EU Data Protection Authorities which can only be beneficial for both and to the coherence of the legal system overall.

In the US, while in substance the system of protection of personal data and the rules on privacy are different from those of the EU, the fact that the FTC has functions relating to both the protection of competition and of privacy has certainly been an advantage in terms of transferring learnings, in particular as to the rigour of investigation and how to produce enforcement decisions which withstand judicial scrutiny, from the area of competition law with a longer enforcement history to the relatively younger area of privacy law. A similar learning is possible in Europe, where competition law also has a longer and more intense history of fining than data protection law. Competition authorities thus have accumulated knowledge on the general preventive effect of fines as well as on how to withstand judicial scrutiny which is very useful for data protection authorities. It is therefore to be hopped that DPAs and Competition Authorities will develop intense relations of mutual inspiration, learning and cooperation. They will after all also often be dealing with the same "clients" in their investigations and enforcement activities.

The duty of DPAs to impose a fine

According to Art. 83 (1) GDPR, the decision of the supervisory authorities to impose fines must be guided by the principles of effectiveness, proportionality and the objective of dissuasion. The concepts of effectiveness and dissuasion merge into each other and cannot be separated from one another. Article 83 (1) GDPR sets out the clear objective that the fine alone must be sufficient to ensure effective sanctioning of data protection breaches with a sufficient dissuasive effect. In particular, the supervisory authorities are therefore prohibited

[9]http://www.bundeskartellamt.de/SharedDocs/Publikation/EN /Press Releases/2017/19_12_2017_Facebook.pdf?__blob=publicationFile&v=3 .

from making the determination of the amount of the fine dependent on any claims for compensation under Art. 82 GDPR. It is also prohibited to them to systematically refrain from a fine. The DPAs can only abstain from a fine in the two cases expressly mentioned in recital 148 GDPR, namely in case of a "*minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person*." Under the wording of Art. 83 (2) GDPR, it is only at the discretion of the supervisory authority to impose a fine "*in addition to, or instead of*" of another supervisory measure under Article 58 (2) (a)-(h) GDPR. This decision must be based on the principle of effectiveness and deterrence. It must always be the goal to give controllers and processors an effective incentive to act lawfully. As a rule, it will not be sufficient to limit the action in case of non-compliance to another supervisory measure or a fine alone. The apodictic wording of Article 83 (2) 1 GDPR ("*Fines ... shall be imposed*"), as well as the wording of recital 148, S. 1 GDPR, make this clear. Recital 148 S. 1 GDRR allows for the a contrario argument because in only mentions two specific two situations in which the DPA can abstain from fining, thus obliging to conclude that if these situations are not present, a fine must be imposed. In its Guidelines, the Art. 29 Working party even states, to be absolutely clear, that "*Recital 148 GDPR does not contain an obligation for the supervisory authority to always replace a fine by a reprimand in the case of a minor infringement ("a reprimand may be issued instead of a fine"), but rather a possibility that is at hand, following a concrete assessment of all 2the circumstances of the case*". So while there is a reduction of discretion to zero in terms of a legal obligation to impose a fine in all cases not falling under the two exceptions in Recital 148 GDPR, there is no reduction to zero of discretion when cases fall under one of these exceptions, and thus also in those cases, depending on circumstances, the DPA can impose a fine. The indirect and wavering language of the Guidelines here reflects the previously different sanctioning traditions of data protection authorities in different Member States. However, the whole purpose of the GDPR being harmonization, and following the general rules of interpretation of EU law, these previously different traditions cannot play a role anymore in the interpretation of the Regulation nor in the practice of application by the DPAs.

Article 83 GDPR however grants the supervisory authorities limited discretion in some respects. These include, in particular, the weighting of the criteria set out in paragraph 2 and the determination of the amount of the fine in accordance with paragraphs 4 and 5. However, according to the case law of the ECJ on competition law in the imposition of fines, the supervisory authorities have no unlimited discretion.[10] On the contrary, they must comply with the general principles of law of the European Union and of the law of the Member States, in particular the principle of equal treatment. As a result, DPAs have a duty to develop an administrative practice for imposing fines in order to deal with similar cases in a similar way. In that regard, particular importance should be attached to the Guidelines of the Article 29 Working Party / the Data Protection Board under Article 70 (1) (k) GDPR. These guidelines, similarly to the Commission's Guidelines on the procedure for fines in competition law, gain quasi-normative meaning, so that deviations from the guidelines will be justiciable. Nothing else will be the case for all other Guidelines of the Data Protection

[10]ECJ 28.4.2010 - T-446/05, ECLI: EU: T: 2010: 165 Para . 140, 142 ff. - Amann & sons and Cousin Filterie / Commission;

Board, given the jurisprudence on the application of Commission Guidelines: In these guidelines, the Commission sets out its future practice on competition law or state aid law in a formally non binding act, namely guidlines. However, on the basis of the principle of equal treatment, the Court has considered such acts as having a self-binding effect. [11]

According to Article 83 (8) and recital 148 GDPR "*reasonable procedural guarantees*" of EU and national law must be respected. In essence, this means that before the decision to impose a fine, the person concerned must be heard ("due process"). In addition, the right to judicial protection must be granted. Its design is the responsibility of the Member States' procedural law. Whether paragraph 8 also lays down the limitation period for infringements relating to the imposition of fines is more than doubtful given the predominantly substantive nature of the limitation period.

The general principles of law of the European Union require that fines are motivated and justified on the basis of the method of calculation used, and this in such a way as to allow the addressee to comply and if necessary to seek judicial remedy.[12] The statement of reasons must mention the aspects relevant to the determination of the amount on which the supervisory authority bases its assessment of the infringement of the GDPR. On the other hand, that does not compel the DPA to give figures as to the way in which the fine is calculated, or even to exercise its discretion solely by the use of mathematical formulas.[13]

Art. 83 (2) 2 GDPR obliges the supervisory authorities in each individual case to fully investigate the matter: For this purpose, the supervisory bodies have at their disposal all the instruments of Art. 58 GDPR. In particular, supervisors can and should, under Article 58 (1) (a) GDPR, oblige the controllers and processors to provide all the information needed to perform their duties. What has been said above on the duty to cooperate and to speak the truth applies a fortiori in this context.

The amount of the fine must be significantly higher than any profit derived from the violation of the GDPR In particular, because a claim for damages under Art. 82 GDPR will never fully apprehend all profits generated, a fine only slightly above the profits will never be enough to provide an effective deterrent. This is so also because the deterrent effect results from the likelihood of an infringement being detected multiplied with the likely size of the fine. Since the likelihood of an infringement being detected remains rather low in the present situation, given in particular the low resources available for enforcement, the fines must be substantially higher in the few cases of non compliance being detected than in a situation in which the likelihood of infringements being detected were higher. Otherwise, the

[11]ECJ 5.4.2006 - T-279/02, ECLI: EU: T: 2006: 103 Para. 82 Degussa / Commission;
[12]ECJ 28.4.2010 - T-446/05, ECLI: EU: T: 2010: 165 Para. 148ff - Amann & Sons and Cousin Filterie / Commission;
[13]ECJ 28.4.2010 - T-446/05, ECLI: EU: T: 2010: 165 Para. 226ff - Amann & Sons and Cousin Filterie / Commission;

deterrent effect of the fines under GDPR, being a factor of likelihood of being detected times size of fine if detected, would become so low that it would not provide sufficient incentive to comply with the GDPR. If DPAs were substantially better equipped with staff and technical ressources to detect non-compliance, the fines could be lower. It is thus in the hands of Governments and Parliaments in Member States to equip their data protection authorities in such a way that the likelihood of detection of non-compliance increase if they would like to see low fines applied in individual fining decisions, the number of which would then however have to increase (absent an increase of systemic compliance).

The poor economic situation of the controller or processor, according to recital 148 S. 2 GDPR, is irrelevant to the amount of the fine, as long as the fine is not imposed on a natural person. This is based on the consideration that otherwise a controller or processor in economic difficulties could gain illegal and unjustified competitive advantages from illegal behaviour. Recital 150 sentence 4 also must be read in this way.[14]

Economic concerns can never be justification for disregarding provisions of the GDPR which serve to protect positions of fundamental rights.

Considerations on the amounts of the fine

In all cases the amount of the fine must be based on the principle of proportionality. The criteria for this purpose as set out in Art. 83 (2) GDPR are further detailed by the Guidelines, in the alphabetical order of Art. 83 (2) GDPR.

Subparagraph (a) lays down certain legal and factual criteria as the basis for determining the amount of the fine, which the supervisory authority must take into account in each individual case. Due to the conceptual breadth of these criteria and given the existence of the "catch-all clause" in point (k), the "*nature*" and "*seriousness*" of the infringement cannot be conclusively defined. The "*severity*" of the infringement may depend on the effect or consequences of the infringement on the person concerned, i.e. whether an injury resulted, for example, in a particular exposure of the data subject in a narrower group of people or even the public, and whether the violation can be reversed or not. With regard to the purpose of the processing, for example, the question may arise as to whether the cause or purpose of the processing was a lawful or unlawful one. In this regard, the Guidelines refer to Guidelines on purpose limitation of 2 April 2013.[15]

According to the Guidelines, the number of data subjects concerned may be an important indicator of systemic errors and a lack of proper data protection routines. The fine does not depend on proof of a causal link between the infringement and the damage, but the amount of the damage and the duration of the infringement are criteria to be taken into account.

[14]See also ECJ, 06.29.2006 - C-308/04 P, ECLI: EU: C: 2006: 433 and ECJ 28.4.2010 - T-446/05, ECLI: EU: T: 2010: 165 Para 198 ff;
[15]Guidelines on purpose limitation of 2 April 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/ 2013 / wp203_en.pdf;

The wording of Article 82 (2) 2 GDPR ("*due regard*"), does not require to either establish intent or negligence in order to impose a fine at all: However, point (b), which refers to the "*intentional or negligent character of the infringement*", makes it possible to take account of the degree of fault on the part of the controller or processor. In that regard, the question arises as to which fault of which person should be assigned to a legal person. The GDPR does not require the attribution of a fault within the meaning of the law of damages. The right standard is rather an administrative law *sui generis* standard. To require an organ fault, i.e. of the board or the CEO, is not necessary according to the wording. The deliberate or negligent conduct of a manager, a person responsible for processing or even the person entrusted with the specific processing operation will also have to be taken into account, depending on the circumstances of the specific case. However, the allegation against the controller or processor becomes all the more serious and thus the higher the fine, the more signs of organizational negligence (and a fortiori of intent) can be found and the more this degree of fault can be attributed to organs of the company or high managers, rather than merely to the possibly unforeseeable or unavoidable misconduct of an individual not having high responsibilities. The instruction of an organ for unlawful processing is regularly regarded as intent under the guidelines. Given the principle that the business man must know the law, and thus take measures to ensure compliance with the law in the company, and given the now numerous actions for awareness raising and offers to ensure compliance with the GDPR in the markets, it is hard to imagine a constellation with repeated infringements of the GDPR without at least negligence present.

If controllers or processors have doubts about the legality of processing, they need to remove these doubts or stop processing until the doubts are removed. Not taking any action in such a situation constitutes deliberate acceptance of potentially breaking the GDPR and thus certainly gross negligence, if not intent. According to the guidelines, the scarcity of funds in the implementation of the rules cannot excuse non-compliance. Signs of intent are unlawful processing despite previous notices by data protection officers or contrary to existing data protection rules adopted within the company. Examples included in the guideline are acquiring data from employees of a competitor in order to discredit it; modification of data in order to claim goal fulfilment, such as related to waiting periods in hospitals; trading data asserting that they would consent without regard to data subjects' statements about how their data should be used.

Negligence shall be considered under the Guidelines if existing data protection policies of the Company have not been read or followed or no data protection rules have been adopted by the Company in the first place (this can also amount to intent in terms of deliberate acceptance of the possibility of non-compliance with the GDPR). Equally, the disclosure of data without checking the absence of personal data indicates negligence according to the Guidelines, as do deficient or late technical updates of programmes or processes. It is fair to say that the Guidelines qualify as negligence a number of constellations which under national administrative or even criminal law would be qualified as intent, in particular under the category of deliberately accepting that it is possible that the law is broken.

Article (83) 2 (c) GDPR sets an incentive for controllers and processors to stop infringements committed as soon as possible, immediately reverse practice and make up for damages. In this case, the concept of damage is not exclusively related to a financial loss. A controller or

processor must also strive to make up for impairments of non-financial nature in order to benefit. Although not explicitly mentioned by the wording, the supervisory authority will conversely have to take into account that no efforts were made to make amends.

The timely and intensive efforts of the controller for "repairs" should, according to the Guidelines, play a role in the determination of the fine, as well as the fact that other involved persons or processors were informed and thus further damage was prevented.

A leniency rule for those admitting an illegal behaviour first, as it exists in competition law, is not contained in the Guidelines so far. In view of the diverse modern constellations of co-controllers or processors in the digital economy, it could be very useful. This is so because leniency, if well applied, facilitates and intensifies enforcement and thus increases the general preventive effect of fines, which are a factor of likelihood of noncompliance being detected times amount of the fines. This presupposes, of course, that leniency is only granted if an actor who accuses itself will also provide substantial information allowing to pursue successfully another or even better more than one other actors who have committed infringements[16] of the GDPR. This will often be possible in constellations of cooperation between processors and controllers or co-controllers, constellations which are increasingly common in the world of the cloud and complex divisions of labour relating to the treatment of personal data.

Letter (d) provides that "*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*" shall be taken account of in the calculation of the fine. Its regulatory content is partly reflected in letter (b), since the determination of the degree of fault will in most cases correspond to the "*degree of responsibility*". Letter (d) gains own significance in addition to letter (b) insofar as it refers to the special provisions for data protection through technology design and privacy-friendly default settings and data security, namely Articles 25 and 32 GDPR. The technical-organizational relevance of these rules goes beyond the simple legal category of intent and negligence. Only by incorporating these provisions into the sanctioning catalogue a real economic incentive to invest in privacy by design and by default is created, as serious and comprehensive investment in this area can significantly reduce the fine. The Guidelines also include in this context the application of organizational measures by the management referred to in Article 24 GDPR. Relevant industry standards and codes of conduct (Art. 40 GDPR) serve to determine best practices to meet.

Letter (e) makes "*relevant previous infringements by the controller or processor*" an aggravating circumstance and thus adds an additional incentive to lawful behaviour. The pedagogical, future-oriented approach of the GDPR is particularly evident here. Moreover, criterion (e) should also be taken into account when a controller selects a processor, although its previous breaches of the GDPR are known or should have been known to the controller, for example because they have already cooperated or the previous breaches are public knowledge. This also results from Art. 28 (1) GDPR, which provides that "*the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this*

[16]See http://ec.europa.eu/competition/cartels/leniency/leniency.html;

Regulation and ensure the protection of the rights of the data subject." Intention or negligence in disregard of this statutory duty of care and scrutiny when selecting a processor should clearly be an aggravating circumstance leading to higher fines for the controller.

According to the Guidelines, the question to be considered in particular is whether the controller or processor has previously committed the same infringement or infringements in a similar manner, for example due to inadequate risk assessment, ignorance of the necessary procedures, negligence in dealing with data subjects, etc. By repetition the breaches referred to in paragraph 4 (2 % of the world turnover of the undertaking concerned) are moved to the higher category (4 % of world turnover of the undertaking concerned) in accordance with paragraph 6, and the guidelines also expressly state this.[17] The Guidelines in Footnote 10 also state in this context that DPAs should observe national rules of limitation. However, where this would put into question the coherent application of the GDPR as EU law, according to the principles of primacy and effectiveness of EU law, the DPAs will have to disregard such rules.

The guidelines are silent on the question whether only violations within the EU or violations outside the EU can be taken as a basis for determining whether a repetition of a previous non-compliance is present. In any case, if an infringement took place outside the EU, but in a context in which EU law was applicable, e.g. pursuant to an adequacy decision such as the EU – US Privacy Shield or due to the large geographic applicability of the Regulation, such violations are to be included as aggravating circumstance. Only proceeding this way serves the protective purpose and this also if the prior infringement was found by a non EU authority . Likewise, the principle of equal treatment of companies established within and outside the EU, which is within the territorial scope of the Regulation (Article 3 GDRP), supports this interpretation, since it entails the equal treatment of conduct within and outside the EU, as far as it falls under the regulation.

Letter (f) includes the degree of compliance with the obligation of the controllers and processors to cooperate with the supervisory authorities both in order to remedy the infringement and to mitigate any adverse effects in calculating the amount of the fine. For the calculation of the fine itself, knowledge about the turnover of the company as well as its organization and affiliation to other companies is absolutely necessary.

The Guidelines also clarify that co-operation under a legal obligation, such as granting access to the company to the supervisory authority, cannot be taken into account as mitigation in the discretionary assessment of the fine. Only cooperation beyond legal obligation can lead to a reduction of the fine.

Letter (g) gives special consideration, as to the level of the fine, to the "*categories of personal data affected by the infringement.*" These are, in particular, the categories referred to in Articles 8-10 GDPR, thus data of children and sensitive data. In addition, the Guidelines cite, as discretionary criteria, the direct or indirect identification of persons; Data whose dissemination directly causes harm or suffering to individuals without falling under Articles 9 or 10 GDPR; and whether data was under protection, such as encryption of data, or not.

[17]Point III (a), in Fn 9 of the Guidelines;

Article 33 (1) GDPR requires the responsible persons to notify the supervisory authority of any reported violations of the GDPR without delay. If this is not done, this will have a negative effect on the calculation of the fine under Article 83 (2) (h) GDPR. Without delay in this context will have to be interpreted as on the first occasion once the violation have become known to the responsible person. A strict interpretation is necessary, given the high public interest in such immediate reporting.

The early co-operation of a controller and processor with a DPA beyond what the law requires could give rise to leniency, as it does in Competition law according to the Commission lenience notice.[18] Also under the scope of the GDPR, such a practice of rewarding whistle blowing and early cooperation could lead to increased degrees of compliance. In this context future Guidelines should provide specific assessment criteria and procedures in accordance with Article 70 (1) (k) GDPR. The present Guidelines make it clear that compliance with the legal obligation alone does not lead to a reduction in the fine, and that negligent, incomplete or late notification can indeed lead to a higher fine and cannot be considered minor. This problem is at issue in an investigation concerning the US Transportation Company Uber,[19] on which the Working Party 29 set up a working group on 29. November 2017.[20]

Letter (i) requires earlier instructions by a DPA to have been given to the controller or processor in relation to the same case. The regulation sanctions in this provision the failure to comply with these earlier instructions. Contrary to letter (e), the Guidelines make it clear that this is only a question of the own measures of the acting supervisory authority.

Again, letter (j) is self-explanatory. It forces controllers and processors to adhere to approved codes of conduct and approved certification procedures or conditions of certification under Articles 24 (3), 28 (5) and 32 (3) GDPR. The Guidelines clarify that although codes of conduct under Art. 40 (4) GDPR must provide for monitoring procedures, the tasks and powers of the supervisory authorities remain unaffected (see also Art. 41 (2) (c) and 42 (4) GDPR). According to the Guidelines, non-compliance with the codes of conduct or certification procedures may also demonstrate intent or negligence.

As already explained, point (k) is a fall back which allows the supervisory authority to fully exercise its discretion, thus to take due account of all the circumstances of the individual case. The exemplary financial benefit of a violation will have to correspond to a mathematical value, which in turn must be related to a specific personal date. As an example of a possible way to calculate the value of a record about a person, for example, in a social network, the company value is divided by the number of members of that network. The Guidelines make it clear that profits from violations in any case give rise to a fine.

[18]Communication from the Commission concerning the adoption and reduction of fines in cartel cases, OJ 2006 C 298, 17; see also http://ec.europa.eu/competition/cartels/leniency/leniency.html;
[19] ECJ 20.12.2017 Case C-434/15 ECLI:EU:C:2017:981 Asociación Profesional Elite Taxi v Uber Systems Spain SL;
[20] see http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083;

Cumulation of infringements and the determination of "the undertaking"

If a controller or processor has committed a number of different infringements in the same processing operation or, in the case of 'linked processing operations', to several provisions of the GDPR, the total amount of the fine is limited to the amount for the most serious infringement. The purpose of this rule is also to clarify that the quantitatively increased disregard for the provisions of the GDPR is particularly in need of sanction.[21] In practical terms, this means that the fine must be increased, but cannot exceed four per cent (para 5).

The term "*linked processing operations*" is neither legally defined nor is it used elsewhere in the GDPR. However, according to the purpose of paragraph 3, the term must be interpreted strictly, otherwise the deterrent effect of Article 83 GDPR would be undermined. Furthermore, a narrow interpretation of the "*linked processing operations*" supports the narrow interpretation of the 'same' processing operations. If these relate to the identical processing operation, this cannot be undermined by an endless interpretation of the connected processing operations. A combination of processing operations is conceivable through several criteria, namely the identity of the data subject, the identity of the purpose of the processing, the nature of the processing operations themselves and the temporal proximity of various processing operations. In order to be able to substantiate a connection within the meaning of para. 3, it is not sufficient for only one of these criteria to be met. At least the identity of the data subject and the purpose of the processing must normally be available in order to affirm a relationship. An example of this is a social network that creates secret profiles based on personal characteristics and their use and resells sections of this profile, to an insurance broker or a company from another sector. Here the processing operations concern different purposes, so that a connection within the meaning of paragraph 3 would not exist. Otherwise, the profit of the social network from all sales transactions could be so high that a single fine within the meaning of para. 3 would no longer have a deterrent effect.

In spite of the cap in paragraph 3, when calculating the total amount, each individual infringement and the amount of each fine under paragraph 2 (a) must be taken into account. The GDPR has been infringed on several occasions in such a case. Therefore, the total amount of the fine will in any event be higher than if only a single infringement had been committed.

Decisive in determining the amounts of the fines will be the delineation of the "undertaking" within the meaning of Art. 83 (4) and (5) GDPR.

On the one hand, Art. 4 No. 18 GDPR should be taken into consideration. According to this, an "*enterprise*" is "*a natural or legal person engaged in an economic activity, regardless of its legal form, including partnerships or associations regularly engaged in economic activity*". On the other hand, recital 150, sentence 3 GDPR, specifically for the imposition of fines, relies on the concept of Articles 101 and 102 TFEU. According to the functional concept of enterprise governed by competition law, an undertaking is any entity engaged in an economic activity, regardless of its legal form and type of financing. In this respect, the

[21]See also ECJ 28.4.2010 - T-446/05, ECLI: EU: T: 2010: 165 Para 160 - Amann & Sons and Cousin Filterie / Commission;

economic unit is decisive, irrespective of whether it consists of several natural or legal persons.[22] According to the case-law of the European Court of Justice, this leads to liability of the parent company for misconduct of its subsidiaries, if they "essentially" follow their instructions due to economic, legal and organizational links.[23] In this respect, a determining factor is that it is suspected in any case if the parent company holds all the shares of the subsidiary.[24] Moreover, according to the concept of competition law, a natural person can also be an undertaking, namely if he or she is conducting a commercial business.

Fines until the entry into force of the GDPR

To close these reflections, let us look back at the fining practices before the entry into force of the GDPR. This is not to suggest that this should in any way be a baseline for future practice. On the contrary, practice based on the GDPR needs to rather align with competition law, not with past practice. Therefore, this is rather a warning on diversity and an encouragement to install from the outset a rigorous and coherent practice of fining.

The highest individual fines imposed in Europe in data protection matters have been those of the Italian Data Protection Authority with a maximum of 5.88 million euros.[25] This is followed by the former Financial Services Authority in London, which oversees compliance with privacy rules by banks and insurance companies. It has fined more than £ 2 million on several occasions.[26] The highest fine in Germany so far imposed on data protection amounted to 1.5 million euros.[27] In terms of the number of individual fining decisions, the data protection authorities most active in recent years, have been those of Spain, the United Kingdom and France.[28] The US FTC fines companies for failing to comply with EU Safe

[22]ECJ 10.9.2009 - C-97/08 P, ECLI: EU: C: 2009: 536 = ECR 2009, 816 Para. 55 - Akzo Nobel / Commission;
[23]ECJ 10.9.2009 - C-97/08 P, ECLI: EU: C: 2009: 536 = ECR 2009, 816 Para 58f - Akzo Nobel / Commission;
[24]ECJ 10.9.2009 - C-97/08 P, ECLI: EU: C: 2009: 536 = ECR 2009, 816 Para 60f - Akzo Nobel / Commission;
[25]http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6009876, for context see http://www.garanteprivacy.it/web/guest/home/docweb/- / docweb-display / docweb / 6072330 and https://iapp.org/news/a/garante-issues-highest-eu-sanction-on-record/
[26]See, for example, the fines totalling £ 3 million against companies of the HSBC Group of 17 July 2009, https://www.fca.org.uk/publication/final-notices/hsbc_actuaris0709.pdf and https: // www.fca.org.uk/publication/final-notices/hsbc_inuk0907.pdf and https://www.fca.org.uk/publication/final-notices/hsbc_ins0709.pdf ; and of 2,275 million pounds against Zurich Insurance of August 19, 2010, https://www.fca.org.uk/publication/final-notices/zurich_plc.pdf
[27]The fine was against supermarket chain Lidl and led to the dismissal of the Germany boss of the company, see press release of the Interior Ministry of Baden- Wuerttemberg v. 11.7.2008 "Data protection supervisory authorities impose heavy fines on Lidl distribution companies for serious data breaches"; http://www.sueddeutsche.de/wirtschaft/lidl-muss-zahlen-millionen-strafe-fuer-die-schnueffler-1.709085 and http://www.faz.net/aktuell/wirtschaft/unternehmen/datenschutz-affaere- lidl-delaulter-germany-chef-1783052.html;
[28]https://www.cnil.fr/fr/les-sanctions-prononcees-par-la-cnil ; and https://www.cnil.fr/fr/recherche/sanctions;

Harbour and other public assurances to protect customer privacy, sometimes in excess of $ 20 million.[29]

In Spain, the highest fine in data protection so far amounted to 1.2 million euros.[30] The Spanish Data Protection Authority has in the three years 2015-17 imposed fines in 1702 cases, resulting in a cumulated amount of 44,894,956 €.[31] The data protection authority of Spain reports in detail about the sanction practice.[32]

In the UK, the highest fine ever imposed by the DPA was £ 400,000[33]. Fines under the jurisdiction of the Financial Services Authority (now the Financial Conduct Authority) quickly exceed the one million mark, when it comes to protecting personal (financial) data in the jurisdiction of that authority.[34]

In comparison, fines in competition law reach billions, for example 2,42 billions Euros in the recent Google case.[35] The legal basis in competition law allows maximum fines of up to 10% of world turnover,[36] the GDPR only 4% of world turnover of the undertaking concerned. Within this important difference, however, there should be a relative approximation of fines between the two legal bases, in line with the overall principle of coherence in the law, in particular against the background of the common purpose of general and special prevention of both legal bases and the high primary law position of data protection as a fundamental right in the digital world.

It is to be hoped that starting from Article 70 (1) y GDPR, the Data Protection Board will set up a register not just of cases dealt with in the Data Protection Board, but of all decisions with fines imposed on the basis of the Regulation, very soon after the entry into force of the Regulation, in order to bring about the transparency necessary in the rule of law and for the coherent application of the Regulation, in particular Art. 58 and 83 GDPR. Until then, there is nothing left to do to gain transparency but to consult individual data protection authorities or use private overview tools, such as the PWC Privacy and Security Enforcement Tracker.[37] An official common database of decisions under the GDPR is just as indispensable for specific

[29]Google paid a total of $ 22.5 million to the FTC following a December 2012 agreement, https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225 -million-settle-ftc-charges-it-misrepresented;
[30]PS / 0082 / 2017th Facebook Inc from 21/08/2017, http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2017/common/pdfs/PS-00082-2017_Resolucion-de-fecha-21-08-2017_Art-ii-culo-4-5-6-7- LOPD.pdf;
[31]Letter to the author by the Spanish DPA;
[32]http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/memorias-ides-idphp.php;
[33]See details at https://ico.org.uk/action-weve-taken/enforcement/?facet_type=Monetary+penalties&facet_sector=&facet_date=&date_from=&date_to=;
[34]https://www.fca.org.uk/news/news-stories/2014-fines;
[35]Google decision of the European Commission of 27. June 2017, http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39740;
[36]Article 23 (2) of Council Regulation (EC) No 1/2003 of 16 December 2002 implementing the competition rules set out in Articles 81 and 82 of the Treaty;
[37]PWC Privacy and Security Enforcement Tracker 2016, see https://www.pwc.co.uk/services/legal-services/ services / cyber-security / privacy-and-security-enforcement-tracker.html;

and general prevention and coherent application as is good public relations work, communicating fining decisions and their motivation in the daily press, trade press and social services.[38]

[38]see last good example of ICO's intense press work in the UK on the 400,000-pound fine in the Carphone case, https://ico.org.uk/about-the-ico/news-and-events/news-and- blogs / 2018/01 / carphone-warehouse-fined-400-000-after-serious-failures-placed-customer-and-employee-data-at-risk/;

Conclusion

With the GDPR, data protection does not only move from a directive to a regulation but also from low (or no) fines to high fines. Seen together, the change of the legal form of the instrument, the setting up of a Data Protection Board with the power to take binding decisions and the introduction of high fines for noncompliance, clearly expresses the will of the legislator to make sure that the rules of the GDPR are fully and coherently applied across Europe in this new age of digitalisation and pervasive personal data processing. The DPAs are entrusted with the duty to ensure this and have obtained substantial new powers for this purpose, comparable to those of competition authorities. The Competition authorities have a long experience in rigorous enforcement against non-compliance. The experience in competition law is that high fines are necessary to better compliance, as only high fines bring about the necessary deterrent against non-compliance. DPAs have an interest to learn from this history of enforcement and fining in competition law. Much of the jurisprudence on competition law fines will mutatis mutandis in any case be applied to data protection by the ECJ. It is now time for Data Protection Authorities to acquire the resolve necessary to stand through complex investigations, impose high fines with a strong deterrent effect and to stand through protracted judicial review battles. This requires skills of leadership and staff competences found today in competition authorities and public prosecutors offices, for example. The DPAs can acquire these skills from there, either by systematic cooperation and training, or by systematic recruitment of staff with experience in legal investigations subject to judicial review, or both.