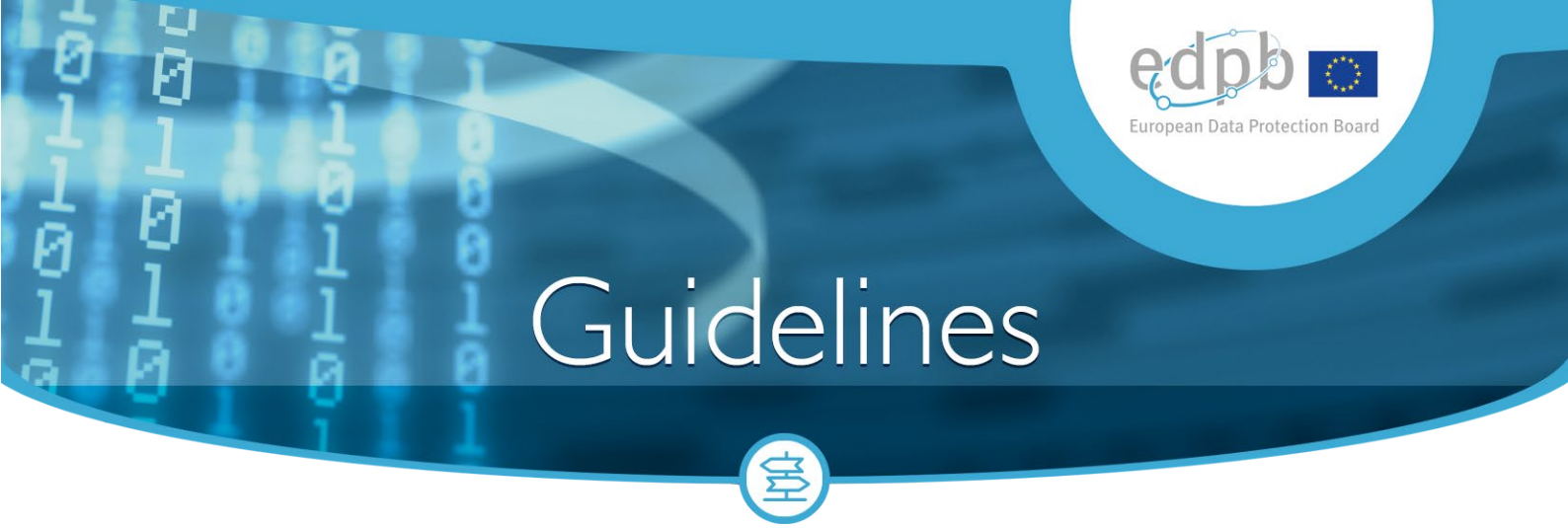


Guidelines 04/2022 on the calculation of administrative fines under the GDPR

Version 1.0

Adopted on 12 May 2022

Executive Summary

The European Data Protection Board (EDPB) has adopted these guidelines to harmonise the methodology supervisory authorities use when calculating of the amount of the fine. These Guidelines complement the previously adopted Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679 (WP253), which focus on the circumstances in which to impose a fine.

The calculation of the amount of the fine is at the discretion of the supervisory authority, subject to the rules provided for in the GDPR. In that context, the GDPR requires that the amount of the fine shall in each individual case be effective, proportionate and dissuasive (Article 83(1) GDPR). Moreover, when setting the amount of the fine, supervisory authorities shall give due regard to a list of circumstances that refer to features of the infringement (its seriousness) or of the character of the perpetrator (Article 83(2) GDPR). Lastly, the amount of the fine shall not exceed the maximum amounts provided for in Articles 83(4) (5) and (6) GDPR. The quantification of the amount of the fine is therefore based on a specific evaluation carried out in each case, within the parameters provided for by the GDPR.

Taking the abovementioned into account, the EDPB has devised the following methodology, consisting of five steps, for calculating administrative fines for infringements of the GDPR.

Firstly, the processing operations in the case must be identified and the application of Article 83(3) GDPR needs to be evaluated (**Chapter 3**). Second, the starting point for further calculation of the amount of the fine needs to be identified (**Chapter 4**). This is done by evaluating the classification of the infringement in the GDPR, evaluating the seriousness of the infringement in light of the circumstances of the case, and evaluating the turnover of the undertaking. The third step is the evaluation of aggravating and mitigating circumstances related to past or present behaviour of the controller/processor and increasing or decreasing the fine accordingly (**Chapter 5**). The fourth step is identifying the relevant legal maximums for the different infringements. Increases applied in previous or next steps cannot exceed this maximum amount (**Chapter 6**). Lastly, it needs to be analysed whether the calculated final amount meets the requirements of effectiveness, dissuasiveness and proportionality. The fine can still be adjusted accordingly (**Chapter 7**), however without exceeding the relevant legal maximum.

Throughout all abovementioned steps, it must be borne in mind that the calculation of a fine is no mere mathematical exercise. Rather, the circumstances of the specific case are the determining factors leading to the final amount, which can – in all cases – vary between any minimum amount and the legal maximum.

These Guidelines and its proposed methodology will remain under constant review of the EDPB.

Table of Contents

The European Data Protection Board

Having regard to Article 70(1)(k), (1)(j) and (1)(e) of the Regulation 2016/679/EU 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, (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,[1]

Having regard to Article 12 and Article 22 of its Rules of Procedure,

Having regard to Article 29 Working Party Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP253, which were endorsed by the European Data Protection Board (hereafter "EDPB") at its first Plenary meeting,

HAS ADOPTED THE FOLLOWING GUIDELINES

CHAPTER 1 – INTRODUCTION

1.1 - Legal framework

1. The EU has – with the General Data Protection Regulation (hereinafter referred to as the "GDPR"), which has been applicable since 25 May 2018 – completed a comprehensive reform of data protection regulation in Europe. The Regulation rests on several key components, one being stronger enforcement powers for supervisory authorities. The Regulation imposes a new, substantially increased level of fines, as well as providing for harmonization of fines between Member States.

2. Data controllers and data processors have increased responsibilities to ensure that the personal data of the individuals are protected effectively. Supervisory authorities have powers to ensure that the principles of the GDPR as well as the rights of the individuals concerned are upheld according to the wording and the spirit of the GDPR.

3. Therefore, the EDPB developed guidance to provide a clear and transparent basis for the supervisory authorities' setting of fines. The previously published Guidelines on the application and setting of administrative fines address the circumstances in which an administrative fine would be an appropriate tool and interpret the criteria of Article 83 GDPR in this respect[2].The present Guidelines address the methodology for the calculation of administrative fines. The two sets of Guidelines are applicable simultaneously and should be seen as complementary.

1.2 - Objective

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".

[2] Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679, WP253 (hereinafter referred to as "Guidelines WP253"). Guidelines WP253 were endorsed by the EDPB in its first Plenary meeting, on 25 May 2018. See Endorsement 1/2018, available online here.

4. These Guidelines are intended for use by the supervisory authorities to ensure a consistent application and enforcement of the GDPR and express the EDPB's common understanding of the provisions of Article 83 GDPR.

5. The aim of these Guidelines is to create harmonized starting points as a common orientation, on the basis of which the calculation of administrative fines in individual cases can take place. However, it is settled case law that any such guidance need not be as specific as to allow a controller or processor to make a precise mathematical calculation of the expected fine[3]. It is emphasized throughout these Guidelines that the final amount of the fine depends on all the circumstances of the case. The EDPB therefore envisages harmonization on the starting points and methodology used to calculate a fine, rather than harmonization on the outcome.

6. These Guidelines can be seen as following a step-by-step approach, though supervisory authorities are not obliged to to follow all steps if they are not applicable in a given case, nor to provide reasoning surrounding aspects of the Guidelines that are not applicable.

7. Notwithstanding these Guidelines, supervisory authorities remain subject to all procedural obligations under national and EU law, including the duty to state reasons for their decisions and their obligations under the one stop shop mechanism. In that light, although the supervisory authorities are required to provide sufficient reasoning for their findings in accordance with national and EU law, these guidelines should not be interpreted as requiring the supervisory authority to state the exact starting amount or quantify the precise impact of each aggravating or mitigating circumstance. Moreover, mere reference to these Guidelines cannot replace the reasoning to be provided in a specific case.

8. The Guidelines will be reviewed on an ongoing basis, as practices in the EU and the EEA are developed. It should be noted that, with the exception of Denmark and Estonia[4], supervisory authorities are authorized to issue administrative fines, which are binding if not appealed. Thus, over time, both administrative and judicial practice will further develop.

1.3 - Scope

9. These Guidelines are intended to govern and lay the foundation of the supervisory authorities' setting of fines on an overarching level. The guidance set out applies to all types of controllers and processors according to Article 4(7) and (8) GDPR except natural persons when they do not act as undertakings. This is not withstanding the powers of national authorities to fine natural persons.

10. According to Article 83(7) GDPR, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State. Provided that supervisory authorities have this power on the basis of national law, these Guidelines apply to the calculation of the fine to be imposed on public authorities and bodies, with the exception of Chapter 4.4. Supervisory authorities remain free, however, to apply a methodology similar to the one described in this Chapter. In addition, Chapter 6 is not applicable to the calculation of the fine to be imposed on public authorities and bodies, in case national law provides for different legal maximums and the public authority or body does not act as an undertaking as defined in Chapter 6.2.1.

[3] See, for example, Case C-189/02 P, C-202/02 P, C-205/02 P to C208/02 P and C-213/02 P, *Dansk Rørindustri A/S and others v. Commission*, para. 172 and Case T-91/11, *InnoLux Corp. v. Commission*, para. 88.
[4] See Recital 151 GDPR.

11. The Guidelines cover cross border cases as well as non-cross border cases.

12. The Guidelines are not exhaustive, neither will they provide explanations about the differences between national administrative, civil or criminal law systems when imposing administrative sanctions in general.

1.4 - Applicability

13. According to Article 70(1)(e) GDPR, the EDPB is empowered to issue guidelines, recommendations and best practices in order to encourage consistent application of the GDPR. Article 70(1)(k) GDPR specifies that the Board shall ensure the consistent application of the GDPR and shall, on its own initiative or, where relevant, at the request of the European Commission, in particular draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58 and the setting of administrative fines pursuant to Article 83.

14. In order to achieve a consistent approach to the imposition of administrative fines that adequately reflects all of the principles in the GDPR, the EDPB has agreed on a common understanding of the assessment criteria in Article 83 GDPR. The individual supervisory authorities will reflect this common approach, in accordance with the local administrative and judicial laws applicable to them.

CHAPTER 2 – METHODOLOGY FOR CALCULATING THE AMOUNT OF THE FINE

2.1 - General considerations

15. Notwithstanding cooperation and consistency duties, the calculation of the amount of the fine is at the discretion of the supervisory authority. The GDPR requires that the amount of the fine shall in each individual case be effective, proportionate and dissuasive (Article 83(1) GDPR). Moreover, when setting the amount of the fine, supervisory authorities shall give due regard to a list of circumstances that refer to features of the infringement (its seriousness) or of the character of the perpetrator (Article 83(2) GDPR). The quantification of the amount of the fine is therefore based on a specific evaluation carried out in each case, taking account of the parameters included in the GDPR.

16. For conduct infringing data protection rules, the GDPR does not provide for a minimum fine. Rather, the GDPR only provides for maximum amounts in Article 83(4)–(6) GDPR, in which several different types of conduct are grouped together. A fine can ultimately only be calculated by weighing up all the elements expressly identified in Article 83(2)(a)–(j) GDPR, relevant to the case and any other relevant elements, even if not explicitly listed in the said provisions (as Article 83(2)(k) GDPR requires to give due regard to any other applicable factor). Finally, the final amount of the fine resulting from this assessment must be effective, proportionate and dissuasive in each individual case (Article 83(1) GDPR). Any fine imposed must sufficiently take into account all of these parameters, whilst at the same time not exceeding the legal maximum provided for in Article 83(4)–(6) GDPR.

2.2 - Overview of the methodology

17. Taking into account these parameters, the EDPB has devised the following methodology for calculating administrative fines for infringements of the GDPR.

Step 1	Identifying the processing operations in the case and evaluating the application of Article 83(3) GDPR. **(Chapter 3)**
Step 2	Finding the starting point for further calculation based on an evaluation of **(Chapter 4)** a) the classification in Article 83(4)–(6) GDPR; b) the seriousness of the infringement pursuant to Article 83(2)(a), (b) and (g) GDPR; c) the turnover of the undertaking as one relevant element to take into consideration with a view to imposing an effective, dissuasive and proportionate fine, pursuant to Article 83(1) GDPR.
Step 3	Evaluating aggravating and mitigating circumstances related to past or present behaviour of the controller/processor and increasing or decreasing the fine accordingly. **(Chapter 5)**
Step 4	Identifying the relevant legal maximums for the different processing operations. Increases applied in previous or next steps cannot exceed this amount. **(Chapter 6)**
Step 5	Analysing whether the final amount of the calculated fine meets the requirements of effectiveness, dissuasiveness and proportionality, as required by Article 83(1) GDPR, and increasing or decreasing the fine accordingly. **(Chapter 7)**

2.3 - Infringements with fixed amounts

18. In certain circumstances the supervisory authority may consider that certain infringements can be punished with a fine of a predetermined, fixed amount. It is at the discretion of the supervisory authority to establish which types of infringements qualify as such, based on their nature, gravity and duration. The supervisory authority cannot make such a determination if this is prohibited or would otherwise conflict with the national law of the Member State.

19. The application of a fixed amount to certain types of infringements cannot hamper the application of the GDPR, in particular Article 83 thereof. Moreover, applying fixed amounts does not relieve supervisory authorities from complying with cooperation and consistency (Chapter VII GDPR).

20. Fixed amounts can be established at the discretion of the supervisory authority, taking into account – inter alia – the social and economic circumstances of that particular Member State, in relation to the seriousness of the infringement as construed by Article 83(2)(a), (b) and (g) GDPR. It is recommended that the supervisory authority communicates the amounts and circumstances for application beforehand.

CHAPTER 3 – CONCURRENT INFRINGEMENTS AND THE APPLICATION OF ARTICLE 83(3) GDPR

21. Before being able to calculate a fine based on the methodology of these guidelines, it is important to first consider what conduct (factual circumstances regarding the behavior) and infringements (abstract legal descriptions of what is sanctionable) the fine is based upon. Indeed, a particular case might include circumstances that could either be considered as one and the same or separate sanctionable conducts. Also it is possible that one and the same conduct could give rise to a number of different infringements where the attribution of one infringement precludes attribution of another infringement or can be attributed alongside each other. In other words, there can be cases of concurrent infringements. Depending on the rules of concurrences such can lead to different calculations of fines.

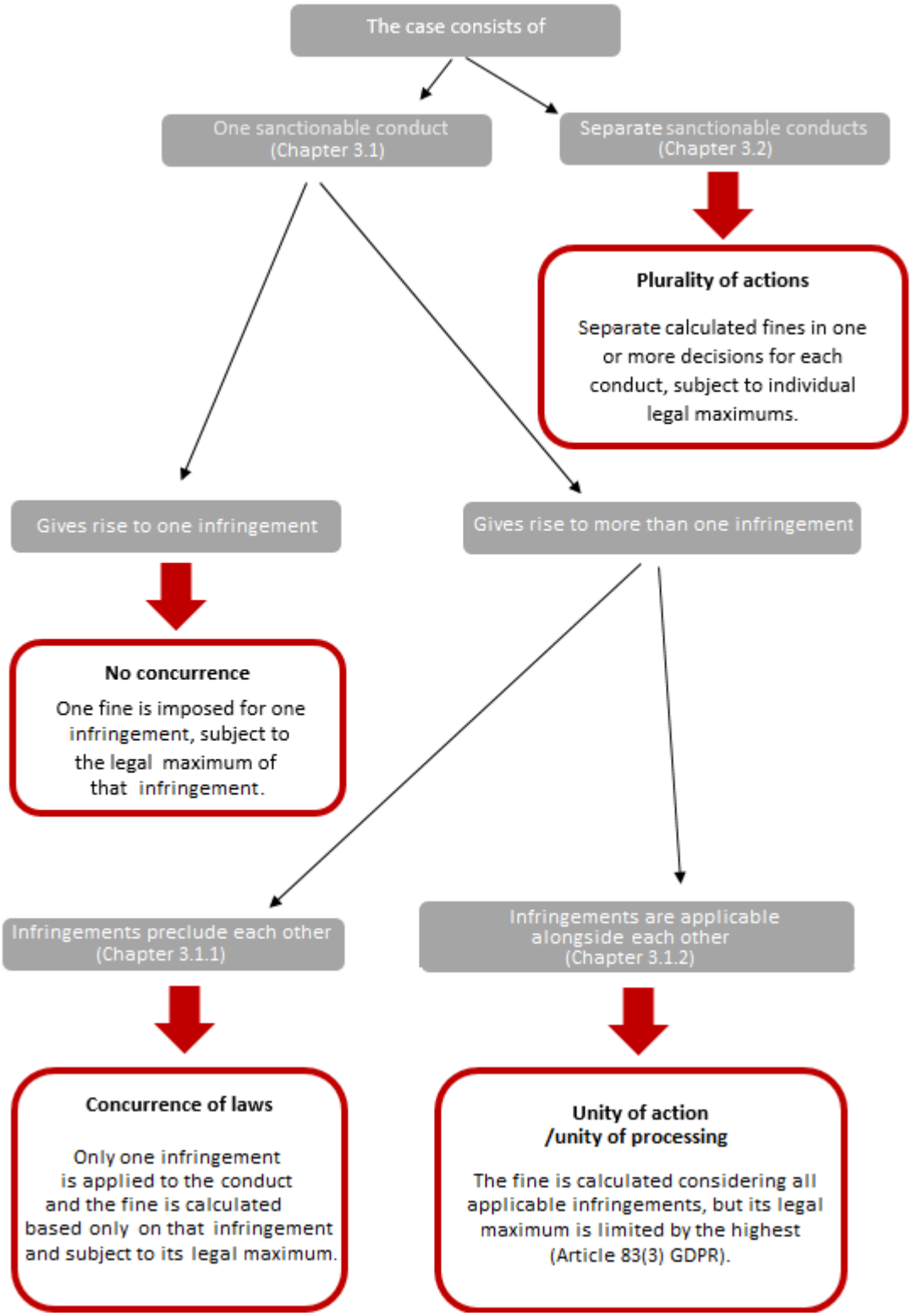
22. Examining the analysis of Member States' traditions of rules on concurrences as outlined in CJEU case-law, [5] and considering the different scopes of application and legal consequences, these principles can be roughly grouped into the following **three categories**:
    - **Concurrence of offences (Chapter 3.1.1)**,
    - **Unity of action (Chapter 3.1.2)**,
    - **Plurality of actions (Chapter 3.2)**.

23. These different categories of concurrences do not conflict with each other, but have different scopes of application and fit into place in a coherent overall system, providing for a logical testing scheme.

24. Therefore, it is important to first establish
    a. Whether or not the circumstances are to be considered as one (**Chapter 3.1**) or multiple sanctionable conducts (**Chapter 3.2**),
    b. In case of one conduct (**Chapter 3.1**), whether or not this conduct gives rise to one or more infringements, and
    c. In case of one conduct that gives rise to multiple infringements, attribution of one infringement precludes the attribution of another infringement (**Chapter 3.1.1**) or whether they are to be attributed alongside each other (**Chapter 3.1.2**).

[5] In particular, see the in-depths analysis of AG Tanchev in case C-10/18, *Marine Harvest*.

Diagram


The case consists of
One sanctionable conduct (Chapter 3.1)
Separate sanctionable conducts (Chapter 3.2)
Plurality of actions
Separate calculated fines in one or more decisions for each conduct, subject to individual legal maximums.
Gives rise to one infringement
Gives rise to more than one infringement
No concurrence
One fine is imposed for one infringement, subject to the legal maximum of that infringement.
Infringements preclude each other (Chapter 3.1.1)
Infringements are applicable alongside each other (Chapter 3.1.2)
Concurrence of laws
Only one infringement is applied to the conduct and the fine is calculated based only on that infringement and subject to its legal maximum.
Unity of action /unity of processing
The fine is calculated considering all applicable infringements, but its legal maximum is limited by the highest (Article 83(3) GDPR).

3.1 - One sanctionable conduct

25. As a first step, it is essential to establish whether there is one and the same sanctionable conduct ("idem") or there are multiple ones in order to identify the relevant sanctionable behavior to be fined. Therefore, it is important to understand what circumstances are considered as one and the same conduct, as opposed to multiple conducts. The relevant sanctionable behavior needs to be assessed and identified on a case-by-case basis. For example in a certain case "the same or linked processing operations" might constitute one and the same conduct.

26. The term "processing operation" is included in Article 4(2) GDPR, where "processing" is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

27. When assessing, "the same or linked processing operations", it should be kept in mind that all obligations legally necessary for the processing operations to be lawfully carried out can be considered by the supervisory authority for its assessment of infringements, including like for instance transparency obligations (e.g. Article 13 GDPR). This is also underlined by the phrase "for the same or linked processing operations", which indicates that the scope of this provision includes any infringement that relates to and may have an impact on the same or linked processing operations.

28. The term "linked" refers to the principle that a unitary conduct might consist of several parts that are carried out by a unitary will and are contextually (in particular regarding identity in terms of data subject, purpose and nature), spatially and temporally related in such a close way that an outside observer would consider them as one coherent conduct. A sufficient link should not be assumed easily, in order for the supervisory authority to avoid infringement of the principles of deterrence and effective enforcement of European law. Therefore, these aspects of relations for a sufficient link need to be assessed on a case-by-case basis and need to be handled restrictively.

Example 1a – The same or linked processing operations
A financial institution requests a credit check from a credit reporting agency (CRA). The financial institution receives this information and stores it in its system.

Although the collection and storage of the creditworthiness data by the financial institution each are by themselves processing operations, they form a set of processing operations that are carried out by a unitary will and are contextually, spatially and temporally related in such a close way that an outside observer would consider them as one coherent conduct. Therefore, the processing operations performed by the financial institution are to be considered as being "linked" and form the same conduct.

Example 1b – The same or linked processing operations
A data broker decides to implement a new processing activity as follows: it decides to collect – as a third party – the consumer transaction history from dozens of retailers without a legal basis, to perform psychometric analysis to predict future behavior of individuals, including political voting behavior, willingness to quit their job and more. In the same decision the data broker decides to not include this procedure in the records of processing activities, not to inform data subjects and to ignore any data subject access requests related to the new processing operations. The processing operations involved in this processing activity form a set of processing operations that are carried out by a unitary will and are

contextually, spatially and temporally related. They are to be considered as being "linked" and forming the same conduct. This also includes the failure to register the processing activity in the records, to inform data subjects and to establish procedures to give effect to the right of access with regard to the new processing operations. These obligations have been infringed for linked processing operations.

Example 1c – Not the same or linked processing operations
(i) A building authority performs a background check of a job applicant. The background check also includes the political affinity, union membership and sexual orientation. (ii) Five days later, the building authority demands from its vendors (sole traders) excessive self-disclosure regarding their business deals with other entities, irrespective of any relevance to the contract with or compliance obligations of the building authority. (iii) Another week later, the building authority suffers a personal data breach. The network of the building authority is hacked – despite having adequate technical and organizational measures in place – and the hacker gains access to a system that processes personal data of citizens that had filed requests with the building authority. Despite the data were adequately encrypted in line with applicable standards, the hacker is able to break it with military decryption technology and sells the data in the dark net. The building authority refrains from notifying the supervisory authority, despite its obligation to do so. The processing operations concerned in this case i.e. the background check, the demands of self-disclosure from vendors and the failure to notify a personal data breach, are not contextually related. Therefore, they are not to be considered "linked", but instead form different conducts.

29. Where it is established that the circumstances of the case form one and the same conduct and give rise to a single infringement, the fine can be calculated based on that infringement and its legal maximum. However, if the circumstances of the case form one and the same conduct, but this conduct gives rise to not only one, but multiple infringements, it must be established whether the attribution of one infringement precludes attribution of another infringement (Chapter 3.1.1) or can they be attributed alongside each other (Chapter 3.1.2). Where the circumstances of the case form multiple conducts, they are to be considered a plurality of actions and handled in line with Chapter 3.2.

3.1.1 - Concurrence of Offences

30. The principle of concurrence of offences (also referred to as "apparent concurrence"[6] or "false concurrence") applies wherever the application of one provision precludes or subsumes the applicability of the other. In other words, concurrence occurs already on the abstract level of statutory provisions. This could either be on grounds of the principle of specialty[7], subsidiarity or consumption, which often apply where provisions protect the same legal interest. In such cases, it would be unlawful to sanction the offender for the same wrongdoing twice[8].

31. In such a case of concurrence of offences, the amount of the fine should be calculated only on the basis of the infringement selected according to above rules (superseding infringement)"[9].

Principle of specialty[10]

[6] See, for example, Austrian Verwaltungsgerichtshof, Ra 2018/02/0123, para. 9.
[7] As assessed in case C-10/18, *Marine Harvest*.
[8] See, for example, Austrian Verwaltungsgerichtshof, Ra 2018/02/0123, para. 7.
[9] As assessed in case C-10/18, *Marine Harvest*.
[10] As assessed in case C-10/18, *Marine Harvest*.

32. The principle of specialty (specialia generalibus derogant) is a legal principle that means that more specific provision (derived from the same legal act or different legal acts of the same force) supersedes a more general provision, although both pursue the same objective. The more specific infringement then is sometimes considered a "qualified type" to the less specific one. Qualified type of infringement might subject to a higher tier of fine, higher legal maximum or more extensive period of limitation.

33. However, sometimes by way of interpretation specialty can also apply, where for reasons of nature and systematics one infringement is considered a qualification of an apparently more specific one, although its wording alone does not explicitly name an additional element.

34. Where instead two provisions pursue autonomous objectives, this constitutes a differentiating factor that justifies the imposition of separate fines. For example, if an infringement of one provision automatically results in an infringement of the other, but the converse is not true, these infringements pursue autonomous objectives.

35. These principles of specialty can only apply, if and as far as the objectives pursued by the concerned infringements are actually congruent in the individual case. As the data protection principles in Article 5 GDPR are established as overarching concepts, there can be situations where other provisions are a concretization of such principle, but not circumscribing the principle in its entirety. In other words, a provision does not always define the full scope of the principle.11 Therefore, depending on the circumstances12, in some cases they overlap in a congruent way and one infringement might supersede the other, while in other cases the overlap is only partial and therefore not fully congruent. As far as they are not congruent, there is no concurrence of offences. Instead, they can be applied alongside each other, when calculating the fine.

Principle of subsidiarity

36. Another form of concurrence of offences is often referred to as the principle of subsidiarity. It applies were one infringement is considered subsidiary to another infringement. This could be either because the law formally declares subsidiarity or because subsidiarity is given for material reasons. The latter can be the case where the infringements have the same objective, but one contains a lesser accusation of immorality or wrongdoing (e.g. an administrative offence can be subsidiary to criminal offence, etc.).

Principle of consumption

37. The principle of consumption applies in cases where the infringement of one provision regularly leads to the infringement of the other, often because one infringement is a preliminary step to the other.

3.1.2 - Unity of action - Article 83(3) GDPR

38. Similar to the situation of concurrence of offences the principle of unity of action (also referred to as "ideal concurrence") applies in cases where one conduct is caught by several statutory provisions, with the difference that one provision is neither precluded nor subsumed by the applicability of the other, because they do not fall in scope of the principles of specialty, subsidiarity or consumption and mostly pursue different objectives.

39. The principle of unity of action was further specified on the level of secondary law in Article 83(3) GDPR in form of a "unity of processing". It is important to understand that Article 83(3) GDPR is limited in its application and will not apply to every single case in which multiple infringements are found to have occurred, but only to those cases where multiple infringements have arisen from "the same or linked processing operations" as explained above[13].

40. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringed several provisions of GDPR, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement (Article 83(3) GDPR).

41. In some special cases a unity of action might also be assumed, where a single action infringes the same statutory provision several times. This could be particularly the case, where circumstances form an iterative and congeneric infringement of the same statutory provision in a close spatial and temporal succession.

> ***Example 2 – Unity of action***
> *A controller sends bundles of marketing e-mails to groups of data subjects in different waves during the course of one day without having a legal ground and thereby infringes Article 6(1) GDPR with one unity of action several times.*

42. The wording in Article 83(3) GDPR does not seem to directly cover this latter case of a unity of action, since "several provisions" are not infringed. However, it would constitute unequal and unfair treatment, if an offender that by one action infringes different provisions that pursue different objectives would be privileged against an offender that infringes with the same action the same provision that pursues the same objective multiple times. To avoid inconsistency of legal principle and in order to comply with the fundamental right on equal treatment in the Charter, in such cases Article 83(3) GDPR shall be applied mutatis mutandis.

43. In case of a unity of action the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement. As regards the interpretation of Article 83(3) GDPR, the EDPB points out that the effet utile principle requires all institutions to give full force and effect to EU law.[14] In this regard Article 83(3) GDPR must not be interpreted in a manner where it would not matter if an offender committed one or numerous infringements of the GDPR when assessing the fine[15].

44. The term "total amount" implies that all the infringements committed have to be taken into account when assessing the amount of the fine and the wording "amount specified for the gravest infringement" refers to the legal maximums of fines (e.g. Articles 83(4)–(6) GDPR).[16] Therefore, although the fine itself may not exceed the legal maximum of the highest fining tier, the offender shall still be explicitly found guilty of having infringed several provisions and these infringements have to be taken into account when assessing the amount of the final fine that is to be imposed[17]. While this is without prejudice to the duty for the supervisory authority imposing the fine to take into account the need for the fine to be proportionate, the other infringements committed cannot be discarded and instead have to be taken into account when calculating the fine.

[13] Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR (hereafter "Binding Decision 1/2021"), para. 320.
[14] Ibid, para. 322.
[15] Ibid, para. 323.
[16] Ibid, para. 325.
[17] Ibid, para. 326.

3.2 - Multiple sanctionable conducts

45. The principle of plurality of actions (also referred to as "Realkonkurrenz", "factual concurrence" or "coincidental concurrence") describes all cases not caught by the principles of concurrence of offences (Chapter 3.1.1) or Article 83(3) GDPR (Chapter 3.1.2).

46. The only reason that these infringements are handled in one decision is by having coincidentally come to the attention of the supervisory authority at the same time without being the same or linked processing operations in the meaning of Article 83(3) GDPR. Therefore, the offender is found to have infringed several statutory provisions and separate fines are imposed according to the national procedure either in the same fining decision or separate fining decisions. Moreover, since Article 83(3) GDPR does not apply, the total amount of the administrative fine may exceed the amount specified for the gravest infringement (argumentum e contrario). Cases of plurality of actions do not pose any reason to privilege the offender with regard to the fining calculation. However, this is without prejudice to the obligation to still comply with the general principle of proportionality.

> ***Example 3 – Plurality of action***
> *After conducting a data protection inspection at the premises of a controller, the supervisory authority finds that the controller failed to establish a procedure for review and continued improvement of its website security, to provide Article 13 information to employees regarding HR data processing and to inform the supervisory authority of a recent data breach regarding its vendor data. None of the infringements is precluded or subsumed by way of specialty, subsidiarity or consumption. Also, they do not qualify as the same processing operation or linked processing operations: they do not form a unity of action, but a plurality of actions. The supervisory authority therefore will find the controller to have infringed by different conducts Articles 13, 32, and 33 GDPR. It will impose in its fining decision individual fines for each, without there being a single legal maximum applicable to their sum.*

CHAPTER 4 – STARTING POINT FOR CALCULATION

47. The EDPB considers that the calculation of administrative fines should commence from a harmonised starting point[18]. This starting point forms the beginning for further calculation, in which all circumstances of the case are taken into account and weighted, resulting in the final amount of the fine to be imposed upon the controller or processor.

48. The identification of harmonised starting points in these Guidelines does not and should not preclude supervisory authorities from assessing each case on its merits. The fine imposed upon a controller/processor can range from any minimum fine until the legal maximum of the fine, provided that this fine is effective, dissuasive and proportionate. The existence of a starting point does not prevent the supervisory authority from lowering or increasing the fine (up to its maximum) if the circumstances of the case so require.

[18] Provided that Guidelines leave sufficient room for the tailoring of an administrative fine to the circumstances of the case, the Court of Justice generally accepts calculations to commence from an abstract starting point. Particularly in joined cases C-189/02 P, C-202/02 P, C-205/02 P to C-208/02 P and C-213/02 P, *Dansk Rørindustri*, but also more recently in case T-15/02, *BASF AG v. Commission*, paras. 120-121; 134, case C-227/14 P, *LG Display Co. Ltd v. Commission*, para. 53 and case T-26/02, *Daiichi Pharmaceutical Co. Ltd v. Commission*, para. 50.

49. The EDPB considers three elements to form the starting point for further calculation: the categorisation of infringements by nature under Articles 83(4)–(6) GDPR, the seriousness of the infringement pursuant to Article 83(2) GDPR and the turnover of the undertaking as one relevant element to take into consideration with a view to imposing an effective, dissuasive and proportionate fine, pursuant to Article 83(1) GDPR. These are outlined in Chapter 4.1, 4.2 and 4.3 below.

4.1 - Categorisation of infringements under Articles 83(4)–(6) GDPR

50. Almost all of the obligations of the controllers and processors according to the Regulation are categorised according to their nature in the provisions of Article 83(4)–(6) GDPR.[19] The GDPR provides for two categories of infringements: infringements punishable under Article 83(4) GDPR on the one hand, and infringements punishable under Article 83(5) and (6) GDPR on the other. The first category of infringements is punishable by a fine maximum of €10 million or 2% of the undertaking's annual turnover, whichever is higher, whereas the second is punishable by a fine maximum of €20 million or 4% of the undertaking's annual turnover, whichever is higher.

51. With this distinction, the legislator provided a first indication of the seriousness of the infringement in an abstract sense. The more serious the infringement, the higher the fine is likely to be.

4.2 - Seriousness of the infringement in each individual case

52. Additionally, the GDPR provides that due regard should be given to circumstances that qualify the seriousness of the infringement in an individual case. More specifically, the GDPR requires the supervisory authority to give due regard to the nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage suffered by them (Article 83(2)(a) GDPR); the intentional or negligent character of the infringement (Article 83(2)(b) GDPR); and the categories of personal data affected by the infringement (Article 83(2)(g) GDPR).

53. The supervisory authority has to review these elements in the light of the circumstances of the specific case and has to conclude – on the basis of this analysis – on the degree of seriousness as indicated in paragraph 61 In this respect, the supervisory authority may also consider whether the data in question was directly identifiable below. Even though they are discussed individually in these Guidelines, in reality these elements are often intertwined and should be viewed in relation to the facts of the case as a whole.

4.2.1 - Nature, gravity and duration of the infringement

54. Article 83(2)(a) GDPR is broad in scope and requires the supervisory authority to carry out a complete examination of all the elements that constitute the infringement and that are suitable to differentiate it from other infringements of the same kind. This assessment should therefore consider the following specific elements:

a) The **nature of the infringement**, assessed by the concrete circumstances of the case. In that sense, this analysis is more specific than abstract classification of Article 83(4)–(6) GDPR. The supervisory authority may review the interest that the infringed provision seeks to protect and the place of this provision in the data protection framework. In addition, the supervisory authority may consider the degree to which the infringement prohibited the effective application of the provision and the fulfilment of the objective it sought to protect.

[19] See in this respect also Guidelines WP253, p. 9.

b) The **gravity of the infringement**, assessed on the basis of the specific circumstances. As stated in Article 83(2)(a) GDPR, this concerns the nature of the processing, but also the scope, purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them," will be indicative of the gravity of the infringement.

i. The **nature of the processing**, including the context in which the processing is functionally based (e.g. business activity, non-profit, political party, etc.) and all the characteristics of the processing.[20] When the nature of processing entails higher risks, e.g. where the purpose is to monitor, evaluate personal aspects or to take decisions or measures with negative effects for the data subjects, depending on the context of the processing and the role of the controller or processor, the supervisory authority may consider to attribute more weight to this factor. Further, a supervisory authority may attribute more weight to this factor when there is a clear imbalance between the data subjects and the controller (e.g. when the data subjects are employees, pupils or patients) or the processing involves vulnerable data subjects, in particular children.

ii. The **scope of the processing**, with reference to the local, national or cross-border scope of the processing carried out and the relationship between this information and the actual extent of the processing in terms of the allocation of resources by the data controller. This element highlights a real risk factor, linked to the greater difficulty for the data subject and the supervisory authority to curb unlawful conduct as the scope of the processing increases. The larger the scope of the processing, the more weight the supervisory authority may attribute to this factor.

iii. The **purpose of the processing**, will lead the supervisory authority to attribute more weight to this factor. The supervisory authority may also consider whether the purpose falls within the so-called core activities of the controller. The more central the processing is to the controller's or processor's core activities, the more severe irregularities in this processing will be. The supervisory authority may attribute more weight to this factor in these circumstances. There may be circumstances though, in which the processing of personal data is further removed from the core business of the controller or processor, but significantly impacts the evaluation nonetheless (this is the case, for example, of processing concerning personal data of workers where the infringement significantly affects those workers' dignity).

iv. The **number of data subjects** concretely but also potentially affected. The higher the number of data subjects involved, the more weight the supervisory authority may attribute to this factor. In many cases it may also be considered that the infringement takes on "systemic" connotations and can therefore affect, even at different times, additional data subjects who have not submitted complaints or reports to the supervisory authority. The supervisory authority may, depending on the circumstances of the case, consider the ratio between the number of data subjects affected and the

[20] By way of example, when analysing the element relating to the "nature of the infringement", the EDPB in its Decision 01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR (hereinafter "Binding Decision 01/2020") noted that the "processing concerned" involved communications by data subjects who deliberately chose to restrict the audience of such communications, and recommended that this aspect be taken into account when evaluating the nature of the processing.

total number of data subjects in that context (e.g. the number of citizens, customers or employees) in order to assess whether the infringement is of a systemic nature.

v. The **level of damage** suffered and the extent to which the conduct may affect individual rights and freedoms. The reference to the "level" of damage suffered, therefore, is intended to draw the attention of the supervisory authorities to the damage suffered, or likely to have been suffered as a further, separate parameter with respect to the number of data subjects involved (for example, in cases where the number of individuals affected by the unlawful processing is high but the damage suffered by them is marginal). Following Recital 75 GDPR, the level of damage suffered refers to physical, material or non-material damage. The assessment of the damage, in any case, be limited to what is functionally necessary to achieve correct evaluation of the level of seriousness of the infringement as indicated in paragraph 61 below, without overlapping with the activities of judicial authorities as tasked with ascertaining the different forms of individual harm.

c) The **duration of the infringement**, meaning that a supervisory authority may generally attribute more weight to an infringement with longer duration. Noting that a given conduct might have been illicit also within the previous regulatory framework, thus adding an additional element to assess the gravity of the infringement. The longer the duration of the infringement, the more weight the supervisory authority may attribute to this factor. If permitted by national law, both the period after the GDPR's effective date and the previous period may be taken into account when quantifying the fine, taking into account the conditions of that framework.

55. The supervisory authority may attribute weight to the abovementioned factors, depending on the circumstances of the case. If not of particular relevance, they may also be considered as neutral.

4.2.2 - Intentional or negligent character of the infringement

56. In its previous guidance, the EDPB stated that "in general, intent includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law."[21] Unintentional in this sense does not equate to non-voluntary.

Example 4 – Illustrations of intent and negligence (from WP253)[22]
"Circumstances indicative of intentional breaches might be 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, for example obtaining and processing data about employees at a competitor with an intention to discredit that competitor in the market. Other examples here might be:
- *amending personal data to give a misleading (positive) impression about whether targets have been met – we have seen this in the context of targets for hospital waiting times,*
- *the trade of personal data for marketing purpose i.e. selling data as 'opted in' without checking/disregarding data subjects' views about how their data should be used.*

Other circumstances, such as 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

[21] Guidelines WP253, p. 11.
[22] Examples quoted directly from Guidelines WP253, p. 12.

manner, failure to adopt policies (rather than simply failure to apply them) may be indicative of negligence."

57. The intentional or negligent character of the infringement (Article 83(2)(b) GDPR) should be assessed taking into account the objective elements of conduct gathered from the facts of the case. The EDPB highlighted that "it is generally admitted that intentional [infringements], demonstrating contempt for the provisions of the law, are more severe than unintentional ones."[23] In case of an intentional infringement, the supervisory authority is likely to attribute more weight to this circumstance. Depending on the circumstances of the case, the supervisory authority may also attach weight to the degree of negligence. At best, negligence could be regarded as neutral.

4.2.3 - Categories of personal data affected

58. Concerning the requirement to take account of the categories of personal data affected (Article 83(2)(g) GDPR), the GDPR clearly highlights the types of data that deserve special protection and therefore a stricter response in terms of fines. This concerns, at the very least, the types of data covered by Articles 9 and 10 GDPR, and data outside the scope of these Articles the dissemination of which causes immediate damages or distress to the data subject[24] (e.g. location data, data on private communication, national identification numbers, or financial data, such as transaction overviews or credit card numbers).[25] In general, the more of such categories of data involved or the more sensitive the data, the more weight the supervisory authority may attribute to this factor.

59. Further, the amount of data regarding each data subject is of relevance, considering that the infringement of the right to privacy and protection of personal data increases with the amount of data regarding each data subject.

4.2.4 - Classifying the seriousness of the infringement and identifying the appropriate starting amount

60. The assessment of the factors above (Chapter 4.2.1–4.2.3) determines the seriousness of the infringement as a whole. This assessment is no mathematical calculation in which the abovementioned factors are considered individually, but rather a thorough evaluation of the concrete circumstances of the case, in which all of the abovementioned factors are interlinked. Therefore, in reviewing the seriousness of the infringement, regard should be given to the infringement as a whole.

61. Based on the evaluation of the factors outlined above, the supervisory authority may find the infringement to be of a low, medium or high level of seriousness. These categories are without prejudice to the question whether or not a fine can be imposed.

- When calculating the administrative fine for infringements of a **low level of seriousness**, the supervisory authority will determine the starting amount for further calculation at a point between 0 and 10% of the applicable legal maximum.

[23] Guidelines WP253, p. 12.
[24] Ibid, p. 14.
[25] Dissemination of private communications and location data can causes immediate damages or distress to the data subject, which has been highlighted by the special protection awarded by the EU Legislator to private communications in Article 7 of the Charter of Fundamental Rights and Directive 2002/58/EC and by the CJEU for location data in certain cases, see joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net et al*, para. 117 and the case law there cited.

- When calculating the administrative fine for infringements of a **medium level of seriousness**, the supervisory authority will determine the starting amount for further calculation at a point between 10 and 20% of the applicable legal maximum.

- When calculating the administrative fine infringements of a **high level of seriousness**, the supervisory authority will determine the starting amount for further calculation at a point between 20 and 100% of the applicable legal maximum.

62. As a general rule, the more severe the infringement within its own category, the higher the starting amount is likely to be.

63. The ranges within which the starting amount is determined remains under review by the EDPB and its members and can be adapted when necessary.

Example 5a – Qualifying the seriousness of an infringement (high level of seriousness)
After investigating numerous complaints about unsolicited calls from customers of a telephone company, the competent supervisory authority found that the telephone company used contact details of its customers for telemarketing purposes without a valid legal basis (infringement of Article 6 GDPR). In particular, the telephone company had offered the names and registered phone numbers of its customers to third parties for marketing purposes. The telephone company did this despite advice against it from the data protection officer, without undertaking any efforts to curb the practice or to offer customers a way of objecting. In fact, the practice had been going on since May 2018 and was still ongoing at the time of the investigation. The telephone company in question operated nationwide and the practice affected all of its 4 million customers. The supervisory authority found that all of these customers had been regularly subjected to unsolicited calls by third parties, without any effective means to stop them.

*The supervisory authority was tasked with assessing the seriousness of this case. As a starting point, the supervisory authority noted that an infringement of Article 6 GDPR is **listed among the infringements of Article 83(5) GDPR** and therefore falls within the higher tier of Article 83 GDPR. Secondly, the supervisory authority assessed the circumstances of the case. In that regard, the supervisory authority attributed significant weight to **nature of the infringement**, as the infringed provision (Article 6 GDPR) underpins the legality of the data processing as a whole. Non-compliance with this provision removes the lawfulness of the processing as a whole. Also, the supervisory authority attributed significant weight to the **duration of the infringement**, which started at the entry into force of the GDPR and had not ceased at the time of the investigation. The fact that the telephone company operated nationwide increased the weight of the **scope of the processing**. The **number of data subjects** involved was considered very high (4 million, offset against a total population of 14 million people), while **the level of damage** suffered by them was considered moderate (non-material damage, in the form of nuisance). The latter assessment was made taking into account the **categories of data affected** (name and phone number). The seriousness of the infringement was increased, however, by the fact that the infringement was committed in contrary to an advice from the data protection officer and, thus, considered **intentional**.*

*Taking all the above into account (serious nature, long duration, high number of data subjects, nationwide scope, intentional nature, vis-à-vis moderate damage), the supervisory concludes that the infringement is considered to be at a **high level of seriousness**. The supervisory authority will determine the starting amount for further calculation at a point between 20 and 100% of the legal maximum included in Article 83(5) GDPR.*

Example 5b – Qualifying the seriousness of an infringement (medium level of seriousness)
A supervisory authority received a personal data breach notification from a hospital. From this notification, it appeared that several staff members had been able to view parts of patients' health files that – based on their department – should not have been accessible to them. The hospital had been working on procedures to regulate access to patient files, and had implemented strict measures for restricted access. That entailed that staff from one department could only access medical information relevant to that specific department. In addition, the hospital had invested in privacy awareness amongst its staff members. However, as it turned out, there were issues concerning the monitoring of authorizations. Staff members that transferred between departments were still able to gain access to the patient files from their "old" departments and the hospital had no procedures in place to match the current position of the staff member with their authorization. Internal investigation by the hospital showed that at least 150 staff members (out of the 3500) had inaccurate authorisations, affecting at least 20,000 of the 95,000 patient files. The hospital could show that in at least 16 instances staff members had used their authorisations to view patient files. The supervisory authority considers that there has been a breach of Article 32 GDPR.

*In assessing the seriousness of the case, the supervisory authority first noted that an infringement of Article 32 GDPR is **listed among the infringements of Article 83(4) GDPR** and therefore falls within the lower tier of Article 83 GDPR. Secondly, the supervisory authority assessed the circumstances of the case. In that regard, the supervisory authority considered that even though the **number of data subjects affected** by the breach was only 16, this could potentially have been 20,000 in the circumstances of the case and even 95,000 given the systemic nature of the issue. Furthermore, the supervisory authority categorized the infringement as **negligent**, but to a low degree, which was considered a neutral factor in the circumstances of this particular case due to the fact that the hospital failed to adopt authorization policies where it surely should have done so but had, otherwise, taken steps to implement strict measures to restrict access. This evaluation was not impacted by the fact that other data protection and security policies were implemented successfully, as the GDPR requires. Lastly, the supervisory authority attributed significant weight to the fact that the patient files include health data, which are **special categories of data** according to Article 9 GDPR.*

*Taking all the above into account (nature of the processing and special categories of data vis-à-vis the number of data subjects actually and potentially affected, the supervisory authority concludes that the infringement is considered to be at a **medium level of seriousness**. The supervisory authority will determine the starting amount for further calculation at a point between 10 and 20% of the legal maximum included in Article 83(4) GDPR.*

Example 5c – Qualifying the seriousness of an infringement (low level of seriousness)
A supervisory authority has received numerous complaints about the way in which an online store handles the right of access of its data subjects. According to the complainants, the handling of their access requests has taken between 4 and 6 months, which is outside the timeframe permitted by the GDPR. The supervisory authority investigates the complaints and finds that the online store responds to access requests a maximum of three months too late in 5% of the cases. In total the store received around 1,000 access requests on an annual basis and confirmed that 950 of these were handled on time. Moreover, the online store had policies in place to safeguard that all access requests were handled correctly and fully. Nevertheless, the supervisory authority concluded that the online store infringed Article 12(3) GDPR and decided to impose a fine.

*During the calculation of the amount of the fine to be imposed, the supervisory authority was tasked with assessing the seriousness of this case. As a starting point, the supervisory authority noted that an infringement of Article 12 GDPR is **listed among the infringements of Article 83(5) GDPR** and therefore falls within the higher tier of Article 83 GDPR. Secondly, the supervisory authority assessed the circumstances of the case. In that regard, the supervisory authority carefully analysed the **nature of the infringement**. Even though the timely right to access to personal data is one of the cornerstones of the data subject rights, the supervisory authority considered that the infringement was of limited seriousness in this respect, given that all requests were handled eventually and with a limited delay. Considering the **purpose of the processing**, the supervisory authority found that the processing of personal data was not the core business of the online store, but still an important ancillary in fulfilling its objective of selling goods online. The supervisory authority considered this to increase the seriousness of the infringement. On the other hand, the **level of damage** suffered by the data subjects was considered minimal, as all access requests were handled within 6 months.*

*Taking all the above into account (nature of the infringement, purpose of the processing and level of damage), the supervisory authority concludes that the infringement is considered to be at a **low level of seriousness**. The supervisory authority will determine the starting amount for further calculation at a point between 0 and 10% of the legal maximum included in Article 83(5) GDPR.*

4.3 - Turnover of the undertaking with a view to imposing an effective, dissuasive and proportionate fine

64. The GDPR requires each supervisory authority to ensure that the imposition of administrative fines is effective, proportionate and dissuasive in each individual case (Article 83(1) GDPR). The application of these principles of European Union law can have far-reaching consequences in individual cases, as the starting points that the GDPR offers for calculating administrative fines apply to micro-enterprises and multinational corporations alike. In order to impose a fine that is effective, proportionate and dissuasive in all cases, supervisory authorities are expected to tailor administrative fines within the entire range available up until the legal maximum. This can lead to significant increases or decreases of the amount of the fine, depending on the circumstances of the case.

65. The EDPB considers that it is fair to reflect a distinction of the size of the undertaking in the starting points identified below and therefore takes into account its turnover[26].However, this does not dismiss a supervisory authority from the responsibility to carry out a review of effectiveness, dissuasiveness and proportionality at the end of the calculation (see Chapter 7). The latter covers all the circumstances of the case, including e.g. the accumulation of multiple infringements, increases and decreases for aggravating and mitigating circumstances and financial/socio-economic circumstances. It is, however, incumbent upon the supervisory authority to ensure that the same circumstances are not counted twice. In particular, supervisory authorities should not, under Chapter 7, repeat the increases or decreases relative to the turnover of the company, but rather revisit their evaluation of the appropriate starting amount.

66. For the reasons outlined above, the supervisory authority may consider adjusting the starting amount corresponding to the seriousness of the infringement in cases where this infringement is committed by an

[26] See also EDPB Binding Decision 1/2021, paras. 411 and 412: "[Insofar] the turnover of an undertaking is not exclusively relevant for the determination of the maximum fine amount in accordance with Article 83(4)-(6) GDPR, but it may also be considered [as one relevant element among others] for the calculation of the fine itself, where appropriate, to ensure the fine is effective, proportionate and dissuasive in accordance with Article 83(1) GDPR." The turnover of the undertaking concerned is further elaborated on in Chapter 6.2 of these Guidelines.

undertaking with an annual turnover not exceeding 2 million euros, an annual turnover not exceeding 10 million euros, or an annual turnover not exceeding 50 million euros[27].

- For undertakings with an annual turnover of ≤ €2m, supervisory authorities may consider to proceed calculations on the basis of a sum down to 0.2% of the identified starting amount.

- For undertakings with an annual turnover of ≤ €10m, supervisory authorities may consider to proceed calculations on the basis of a sum down to 0.4% of the identified starting amount.

- For undertakings with an annual turnover of ≤ €50m, supervisory authorities may consider to proceed calculations on the basis of a sum down to 2% of the identified starting amount.

67. For the same reasons, the supervisory authority may consider adjusting the starting amount corresponding to the seriousness of the infringement in cases where this infringement is committed by an undertaking with an annual turnover not exceeding 100 million euros, an annual turnover not exceeding 250 million euros and an annual turnover not exceeding 500 million euros[28].

- For **undertakings with an annual turnover of €50m up until €100m**, supervisory authorities may consider to proceed calculations on the basis of a sum down to 10% of the identified starting amount.

- For **undertakings with an annual turnover of €100m up until €250m**, supervisory authorities may consider to proceed calculations on the basis of a sum down to 20% of the identified starting amount.

- For **undertakings with an annual turnover of €250m or above**, supervisory authorities may consider to proceed calculations on the basis of a sum down to 50% of the identified starting amount.

68. As a general rule, the higher the turnover of the undertaking within its applicable tier, the higher the starting amount is likely to be. The latter holds particularly true for the largest of undertakings, for which the category of starting amounts has the widest range.

69. Moreover, the supervisory authority is under no obligation to apply this adjustment if it is not necessary from the point of view of effectiveness, dissuasiveness and proportionality to adjust the starting amount of the fine.

70. It should be reiterated that these figures are the starting points for further calculation, and not fixed amounts (price tags) for infringements of provisions of the GDPR. The supervisory authority has the discretion to utilize the full fining range from any minimum fine until the legal maximum, ensuring that the fine is tailored to the circumstances of the case, as the Court of Justice requires in case an abstract starting point is used.

Example 6a – Identifying the starting points for further calculation
A supermarket chain with a turnover of €8 billion has infringed Article 12 of the GDPR. The supervisory authority, based on a careful analysis of the circumstances of the case, decided that the infringement is of a low level of seriousness. To determine the starting point for further calculation, the supervisory authority first identifies that Article 12 GDPR is listed in Article 83(5)(b) GDPR and

[27] These turnover figures are inspired by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. In determining the starting points, the EDPB relies on the annual turnover of the undertaking alone (see Chapter 6 below).
[28] These figures are added to bridge the gap between the highest threshold of the previous paragraph and the turnover threshold identified in Article 83(4)–(6) GDPR.

that, based on the turnover of the undertaking (€8 billion), a legal maximum of €320,000,000,- applies.

Based on the level of seriousness determined by the supervisory authority (low), a starting amount between €0,- and €32,000,000,- should be considered (between 0 and 10% of the applicable legal maximum, see paragraph 61 above). Based on the turnover of the undertaking (€8 billion), the supervisory authority may consider to further reduce this amount to 50% of the identified starting amount corresponding to the seriousness of the infringement.

The supervisory authority considers that – due to the relatively low seriousness of the infringement, offset against the relatively high turnover of the undertaking – a starting amount of €25,000,000,- is considered effective, dissuasive and proportionate. This amount forms the basis for further calculation, which should result in a final amount not exceeding the applicable legal maximum of €320,000,000,-.

Example 6b – Identifying the starting points for further calculation
A start-up dating app with a turnover of €500,000,- is discovered to have sold sensitive personal data of its customers to several data brokers for analytics and thereby infringed Articles 9 and 5(1)(a) of the GDPR. The supervisory authority, based on a careful analysis of the circumstances of the case, decided that the infringement is of a high level of seriousness. To determine the starting point for further calculation, the supervisory authority first identifies that Articles 9 and 5 GDPR are listed in Article 83(5)(a) GDPR and that, based on the turnover of the undertaking (€500,000,-), a legal maximum of €20,000,000,- applies.

Based on the level of seriousness determined by the supervisory authority (high), a starting amount between €4,000,000,- and €20,000,000,- should be considered (between 20 and 100% of the applicable legal maximum, see paragraph 61 above). Based on the turnover of the undertaking (€500,000,-), the supervisory authority may consider to further reduce this amount to 0.2% of the identified starting amount corresponding to the seriousness of the infringement.

The supervisory authority considers that – due to the high level of seriousness of the infringement – a starting amount of €16,000,- is considered effective, dissuasive and proportionate, notwithstanding the low turnover of the undertaking. This amount forms the basis for further calculation, which should result in a final amount not exceeding the applicable maximum of €20 million.

CHAPTER 5 – AGGRAVATING AND MITIGATING CIRCUMSTANCES

5.1 - Identification of aggravating and mitigating factors

71. Following the structure of the GDPR, after having evaluated the nature, gravity and duration of the infringement as well as its intentional or negligent character of the infringement and the categories of personal data affected, the supervisory authority must take account of the remaining aggravating and mitigating factors as listed in Article 83(2) GDPR.

72. With regard to the assessment of these elements, increases or decreases of a fine cannot be predetermined through tables or percentages. It is reiterated that the actual quantification of the fine will depend on all the elements collected during the course of the investigation and on further considerations also linked to previous fining experiences of the supervisory authority.

73. For clarity, it should be noticed noted that each criterion of Article 83(2) GDPR – whether it is assessed under Chapter 4 or this Chapter – should only be taken into account once as part of the overall assessment of Article 83(2) GDPR.

5.2 - Actions taken by controller or processor to mitigate damage suffered by data subjects

74. A first step in determining whether aggravating or mitigating circumstances have occurred, is to review Articles 83(2)(c), which concerns "any action taken by the controller or processor to mitigate the damage suffered by data subjects."

75. As recalled in Guidelines WP253, data controllers and processors are already obliged to "implement technical and organisational measures to ensure a level of security appropriate to the risk, to carry out data protection impact assessments and mitigate risks arising from the processing of personal data to the rights and freedoms of the individuals." However, in case of an infringement, the controller or processor should "do whatever they can do in order to reduce the consequences of the breach for the individual(s) concerned."[29]

76. The adoption of appropriate measures to mitigate the damage suffered by the data subjects may be considered a mitigating factor, decreasing the amount of the fine.

77. The measures adopted must be assessed, in particular, with regard to the element of timeliness, i.e. the time when they are implemented by the controller or processor, and their effectiveness. In that sense, measures spontaneously implemented prior to the commencement of the supervisory authority's investigation becoming known to the controller or processor are more likely to be considered a mitigating factor, than measures that have been implemented after that moment.

5.3 - Degree of responsibility of the controller or processor

78. Following Article 83(2)(d), the degree of responsibility of the controller or processor will have to be assessed, taking into account measures implemented by them pursuant to Articles 25 and 32 GDPR. In line with Guidelines WP253, "the question that the supervisory authority must then answer is to what extent the controller "did what it could be expected to do" given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the Regulation."[30]

[29] Guidelines WP253, p. 12.
[30] Ibid, p. 13.

79. In particular, with regard to this criterion, the residual risk for the freedoms and rights of the data subjects, the impairment caused to the data subjects and the damage persisting after the adoption of the measures by the controller as well as the degree of robustness of the measures adopted pursuant to Articles 25 and 32 GDPR must be assessed.

80. In this respect, the supervisory authority may also consider whether the data in question was directly identifiable and/or available without technical protection[31]. However, it should be borne in mind that the existence of such protection does not necessarily constitute a mitigating factor (see paragraph 82 below). This depends on all the circumstances of the case.

81. In order to adequately assess the above elements, the supervisory authority should take into account any relevant documentation provided by the controller or processor, e.g. in the context of the exercise of their right of defence. In particular, such documentation could provide evidence of when the measures were taken and how they were implemented, whether there were interactions between the controller and the processor (if applicable), or whether there has been contact with the DPO or data subjects (if applicable).

82. Given the increased level of accountability under the GDPR in comparison with Directive 95/46/EC,[32] it is likely that the degree of responsibility of the controller or processor will be considered an aggravating or a neutral factor. Only in exceptional circumstances, where the controller or processor has gone above and beyond the obligations imposed upon them, will this be considered a mitigating factor.

5.4 - Previous infringements by the controller or processor

83. According to Article 83(2)(e) GDPR, any relevant previous infringements committed by the controller or processor must be considered when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine. Similar wording is found in Recital 148 GDPR.

5.4.1 - Time frame

84. Firstly, regard must be given to the point in time when the prior infringement took place, considering that the longer the time between a previous infringement and the infringement currently being investigated, the lower its significance. Consequently, the longer ago the infringement was committed, the less relevance shall be given by the supervisory authorities. This assessment is left at the discretion of the supervisory authority, subject to applicable national- and European law and principles.

85. However, since infringements committed a long time ago might still be of interest when assessing the "track record" of the controller or processor, fixed limitation periods are not to be set to this purpose. However, some national laws do prevent the supervisory authority from considering previous infringements after a settled period. Likewise, certain national laws impose a record deletion obligation after a certain period of time, which prevents the acting supervisory authorities from taking into account these precedents.

86. For the same reason, it should be noted that infringements of the GDPR, since they will be more recent, must be considered as more relevant than infringements of the national provisions adopted for the implementation of Directive 95/46/EC (if national laws allow such infringements to be taken into account by the supervisory authority).

[31] Ibid, pp. 14-15.
[32] Ibid.

5.4.2 - Subject matter

87. For the purpose of Article 83(2)(e) GDPR, previous infringements of either the same or different subject matter to the one being investigated might be considered as "relevant".

88. Even though all prior infringements might provide an indication about the controller's or processor's general attitude towards the observance of the GDPR, infringements of the same subject matter must be given more significance, as they are closer to the infringement currently under investigation, especially when the controller or processor previously committed the same infringement (repeated infringements). Thus, same subject-matter infringements must be considered as more relevant than previous infringements concerning a different topic.

89. For example, the fact that the controller or the processor had failed in the past to respond to data subjects exercising their rights in a timely manner must be considered more relevant when the infringement being investigated refers also to a lack of response to a data subject exercising their rights than when it refers to a personal data breach.

90. However, due account must be taken of previous infringements of a different subject matter, but that were committed in the same manner, as they might be indicative of persisting problems within the controller or processor organization. For example, this would be the case for infringements arising as a consequence of having ignored the advice provided by the Data Protection Officer.

5.4.3 - Other considerations

91. If considering a previous infringement of the national provisions adopted for the implementation of the Directive 95/46/EC, the supervisory authorities must take into account the fact that the requirements in the Directive and the GDPR might differ (if national laws allow such infringements to be taken into account by the supervisory authority).

92. When considering the relevance of a previous infringement, the supervisory authority should take account of the status of the procedure in which the previous infringement was established – particularly of any measures taken by the supervisory authority or by the judicial authority – in accordance with national law.

93. Previous infringements could also be considered when they were found by a different supervisory authority concerning the same controller/processor. For example, the lead supervisory authority dealing with an infringement through the cooperation (one-stop-shop) mechanism in accordance with Article 60 GDPR could take into account infringements previously determined in local cases, by another supervisory authority, concerning the same controller/processor. Likewise, infringements previously determined by the lead supervisory authority could be taken into account when a different authority must handle a complaint lodged with it in cases with only local impacts under Article 56(2) GDPR. Where there is no lead supervisory authority (for example, in case the controller or processor is not established in the European Union), supervisory authorities could also take into account infringements previously determined by another supervisory authority concerning the same controller/processor.

94. The existence of previous infringements can be considered an aggravating factor in the calculation of the fine. The weight given to this factor is to be determined in view of the nature and frequency of the previous infringements. The absence of any previous infringements, however, cannot be considered a mitigating factor, as compliance with the GDPR is the norm. If there are no previous infringements, this factor can be regarded as neutral.

5.5 - Degree of cooperation with the supervisory authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement

95. Article 83(2)(f) requires the supervisory authority to take account of the degree of the controller's or processor's cooperation with the supervisory authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement.

96. Before further assessing the level of cooperation the controller or processor has established with the supervisory authority, it must be reiterated that a general obligation to cooperate is incumbent on the controller and the processor pursuant to Article 31 GDPR, and that lack of cooperation may lead to the application of the fine provided for in Article 83(4)(a) GDPR. It should therefore be considered that the ordinary duty of cooperation is mandatory and should therefore be considered neutral (and not a mitigating factor).

97. However, where cooperation with the supervisory authority has had the effect of limiting or avoiding negative consequences for the rights of the individuals that might otherwise have occurred, the supervisory authority may consider this a mitigating factor in the sense of Article 83(2)(f) GDPR, thereby decreasing the amount of the fine. This may for instance be the case when a controller or processor "has responded in a particular manner to the supervisory authority's requests during the investigation phase in that specific case which has significantly limited the impact on individuals' rights as a result"[33].

5.6 - The manner in which the infringement became known to the supervisory authority

98. Following Article 83(2)(h), the manner in which the infringement became known to the supervisory authority could be a relevant aggravating or mitigating factor. In assessing this, particular weight can be given to the question whether, and if so to what extent, the controller or processor notified the infringement out of its own motion, before the infringement was known to the supervisory authority by – for instance – a complaint or an investigation. This circumstance is not relevant when the controller is subject to specific notification obligations (such as in the case of personal data breaches according to Article 33[34]). In such cases, this notification should be considered as neutral[35].

99. Where the infringement became known to the supervisory authority by, for instance, a complaint or an investigation this element should also, as a rule, be considered as neutral. The supervisory authority may consider this a mitigating circumstance if the controller or processor notified the infringement out of its own motion, prior to the supervisory authority's knowledge of the case.

5.7 - Compliance with measures previously ordered with regard to the same subject matter

100. Article 83(2)(i) GDPR states that "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" must be considered when deciding whether to impose an administrative fine and deciding on its amount.

[33] Guidelines WP253, p. 14.

[34] It should be underlined that a personal data breach does not necessarily imply a GDPR infringement

[35] This is underlined by Guidelines WP253, p. 15.

101. As opposed to Article 83(2)(e) GDPR, this assessment only refers to measures that supervisory authorities themselves have previously issued to the same controller or processor with regard to the same subject matter[36].

102. In this respect, the controller or processor might hold reasonable expectations that compliance with measures previously issued against them would prevent a same subject-matter infringement from taking place in the future. However, since compliance with measures previously ordered is mandatory for the data controller or processor, it should not be taken into account as a mitigating factor per se. On the contrary, a reinforced commitment on the part of the controller or processor in the fulfilment of previous measures is required for this factor to apply as mitigating, e.g. taking additional measures beyond those ordered by the supervisory authority.

103. Conversely, non-compliance with a corrective power previously ordered may be considered either as an aggravating factor, or as a different infringement in itself, pursuant to Article 83(5)(e) and Article 83(6) GDPR. Therefore, due note should be taken that the same non-compliant behaviour cannot lead to a situation where it is punished twice.

5.8 - Adherence to approved codes of conduct or approved certification mechanisms

104. Article 83(2)(j) GDPR states that adherence to codes of conduct pursuant to Article 40 GDPR or approved certification mechanisms pursuant to Article 42 GDPR may be a relevant factor in deciding whether to impose a fine, and the amount of the administrative fine.

105. As recalled by Guidelines WP253, adherence to codes of conduct pursuant to Article 40 GDPR or approved certification mechanisms pursuant to Article 42 GDPR may in some circumstances constitute a mitigating factor. Approved codes of conduct will, according to Article 40(4) GDPR, contain "mechanisms which enable the (monitoring) body to carry out mandatory monitoring of compliance with its provisions." Certain forms of sanctioning non-compliant behaviour may be made through the monitoring scheme, according to Article 41(4) GDPR, including suspension or exclusion of the controller or processor concerned from the code community. Although the supervisory authority can take into account previously imposed sanctions pertaining to the self-regulatory scheme, the powers of the monitoring body are "without prejudice to the tasks and powers of the competent supervisory authority", which means that the supervisory authority is not under an obligation to take into account any sanctions by the monitoring body[37].

106. On the other hand, if failure to comply with the codes of conduct or certification is directly relevant to the infringement, the supervisory authority may consider this an aggravating circumstance.

5.9 - Other aggravating and mitigating circumstances

107. Article 83(2)(k) GDPR gives the supervisory authority room to take into account any other aggravating or mitigating factors applicable to the circumstances of the case. In the individual case there may be many elements involved, which cannot all be codified or listed and which will have to be taken into account in order to ensure that the sanction applied is effective, proportionate and dissuasive in each individual case.

[36] Ibid.
[37] Ibid.

108. Article 83(2)(k) GDPR mentions examples of "any other aggravating or mitigating factor applicable to the circumstances of the case," i.e. financial benefits gained, or losses avoided, directly or indirectly, from the infringement. It is considered that this provision is of fundamental importance for adjusting the amount of the fine to the specific case. In this sense, it is considered that it should be interpreted as an instance of the principle of fairness and justice applied to the individual case.

109. The scope of this provision, which is necessarily open-ended, should include all the reasoned considerations regarding the socio-economic context in which the controller or processor operates, those relating to the legal context and those concerning the market context.

110. In particular, economic gain from the infringement could be an aggravating circumstance if the case provides information about profit obtained as a result of the infringement of the GDPR.

111. Exceptional circumstances that can lead to significant changes in the socio-economic context (e.g. the onset of a serious pandemic emergency that could radically change the way processing of personal data is carried out) could also be considered under Article 83(2)(k) GDPR.

NB: The examples in this Chapter are illustrations of the effect that aggravating and mitigating circumstances may have on the amount of the fine. The increases or decreases mentioned in these imaginary cases cannot be considered precedents or indications of percentages to be used in real life cases.

Example 7a – Weighing aggravating and mitigating circumstances
A sports club used cameras with facial recognition technology at the entrance of one of their locations for the purpose of identifying their clients upon entry. As the sports club did so in contravention of Article 9 GDPR (processing of biometric data without a valid exception), the supervisory authority competent to investigate the infringement decided to impose a fine. Taking into account all the relevant circumstances of the case, the supervisory authority considered this an infringement with a high level of seriousness, and since the sports club had an annual turnover of €150 million, a starting amount of €2,000,000,- (at the very top of the category) was considered appropriate.

However, the same sports club was fined two years earlier for using fingerprint technology at the turnstiles in another location. The supervisory authority decided to take this into account as a repeat offence (Article 83(2)(e) GDPR). In doing so, it attributed weight to the fact that this concerned nearly the same subject matter and the infringement was committed only two years prior. Because of this aggravating factor, the supervisory authority decided to increase the fine in this particular case to €2,600,000,-,[38] not exceeding the applicable legal maximum of €20 million.

NB: The examples in this Chapter are illustrations of the effect that aggravating and mitigating circumstances may have on the amount of the fine. The increases or decreases mentioned in these imaginary cases cannot be considered precedents or indications of percentages to be used in real life cases.

[38] This illustrates that the categories for starting amounts do not limit the supervisory authorities' abilities to take into account aggravating and mitigating circumstances to an amount above or below the categories. As is reiterated in Chapter 4.4, these figures are the starting points for further calculation, and not fixed amounts (price tags) for infringements of provisions of the GDPR. The supervisory authority retains the discretion to utilize the full fining range from a point above €0,- until the legal maximum, ensuring that the fine is tailored to the circumstances of the case.

Example 7b – Weighing aggravating and mitigating circumstances
The operator of a short-term car rental platform suffered a data breach, causing the personal data of its clients to have been vulnerable for a short amount of time. Taking into account all the relevant circumstances of the case, the supervisory authority considered the shortcomings of the operator in securing its platform to infringe Article 32 GDPR, to be an infringement of a low level of seriousness, and since the operator had an annual turnover of €255 million, a starting amount of €260,000,- was considered appropriate.

The compromised personal data included copies of drivers' licences and ID's. For that reason, all clients that suffered from the data breach were forced to reapply for these documents in order to limit the possibility of identity theft. While informing the data subjects of this incident, the operator offered all data subjects assistance in reapplying for these documents with the correct public institutions and created a system to reimburse any fees paid for the application. The supervisory considered this as 'actions to mitigate the damage suffered by data subjects' (Article 83(2)(c) GDPR), which had a mitigating effect on the fine. Given the proactive attitude and the effectiveness of the measures taken by the operator, the supervisory authority decided to lower the fine to €225,000,-,[39] *again not exceeding the legal maximum of €10 million.*

The examples in this Chapter are illustrations of the effect that aggravating and mitigating circumstances may have on the amount of the fine. The increases or decreases mentioned in these imaginary cases cannot be considered precedents or indications of percentages to be used in real life cases.

Example 7c – Weighing aggravating and mitigating circumstances
A small credit rating agency was found to have infringed several provisions safeguarding data subject rights, most notably because it charged its clients a fee for exercising their right to access. The agency did so for all access requests, not just those mentioned in Article 12(5)(a) GDPR. Taking into account all the relevant circumstances of the case, the supervisory authority considered the infringements found to be of a high level of seriousness, and since the agency had an annual turnover of €35 million, a starting amount of €100,000,- was considered appropriate.

However, the supervisory authority considered the fact that the agency was able to profit from the infringement an aggravating circumstance (Article 83(2)(k) GDPR. With a view to counterbalancing the gains from the infringement, while maintaining an effective, dissuasive and proportionate fine in this case, the supervisory authority decided to increase the fine to €130,000,-, not exceeding the applicable legal maximum of €20 million.

The examples in this Chapter are illustrations of the effect that aggravating and mitigating circumstances may have on the amount of the fine. The increases or decreases mentioned in these imaginary cases cannot be considered precedents or indications of percentages to be used in real life cases.

Example 7d – Weighing aggravating and mitigating circumstances
A company was found to have infringed provisions of GDPR, most notably because of selling its database for commercial prospecting to partners containing personal data related to people who did not give their consent to be prospected for commercial purposes.

[39] Please see previous footnote.

Considering all the relevant circumstances of the case, the supervisory authority considered the infringements found to be of a medium level of seriousness, and since the company had an annual turnover of €45 million, a starting amount of €150,000, - was considered appropriate.

Moreover, the authority considered that this was an infringement that benefited the controller because the fact of not having collected the consent of the people for the transmission of their data for the purpose of sending targeting advertising increased the mass of data that it has been able to resell afterwards. Thus, the supervisory authority considered the fact that the agency was able to profit from the infringement an aggravating circumstance (Article 83(2)(k) GDPR).

With a view to counterbalancing the gains from the infringement, while maintaining an effective, dissuasive and proportionate fine in this case, the supervisory authority decided to increase the fine to €200,000, not exceeding the applicable legal maximum of €20 million.

CHAPTER 6 – LEGAL MAXIMUM AND CORPORATE LIABILITY

6.1 - Determining the Legal Maximum

112. As already outlined in the Guidelines WP253, the GDPR does not tag fixed sums to specific infringements. Instead, the GDPR provides for overall maximum amounts[40] and thereby follows the general tradition of EU law on sanctions already established by other legal acts[41].

113. The amounts in Article 83(4)–(6) GDPR constitute the legal maximum and prohibit the supervisory authorities from imposing fines that in their outcome exceed the applicable maximum amounts. In order to determine the correct legal maximum, Article 83(3) GDPR needs to be taken into account[42], where applicable (see Chapter 3.1.2). Each supervisory authority therefore has to ensure that these maximum amounts are not exceeded when calculating fines based on these Guidelines. Depending on the individual case, different maximum amounts may become relevant.

6.1.1 - Static maximum amounts

114. Article 83(4)–(6) GDPR provide for static amounts as a rule and differentiate between infringements of different categories of obligations under the GDPR. As explained above Article 83(4) GDPR allows for fines up to €10 million for infringing the obligations outlined therein, while Article 83(5) and (6) GDPR allow for fines up to €20 million for infringing the obligations outlined in them.

[40] Recital 150 GDPR, second sentence: "This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement."

[41] In particular Article 23(2) of Regulation (EC) No. 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty.

[42] Please see also EDPB Binding Decision 1/2021, para. 326.

6.1.2 - Dynamic maximum amounts

115. In case of an undertaking[43] the fining range may shift towards a higher turnover-based[44] maximum amount. This turnover-based maximum amount is dynamic and individualized towards the respective undertaking in order to achieve the principles of effectiveness, proportionality and deterrence.

116. More specifically, Article 83(4) GDPR allows for a maximum amount of 2% and Article 83(5) and (6) for a maximum amount of 4% of the undertaking's total annual turnover of the previous financial year. The wording of the GDPR requires consideration of the static maximum amount or the dynamic turnover-based maximum amount, "whichever is higher". Consequently, these turnover-based maximum amounts only apply if they exceed the static maximum in the individual case. That is the case when the undertaking's total annual turnover of the previous financial year amounts to more than €500 million[45].

Example 8a – Dynamic maximum
A credit reporting agency (CRA) collects and sells all creditworthiness data of all EU citizens to advertising and retailing companies without a legal basis. The CRA's annual worldwide turnover of the preceding year amounts to €3 billion. Here, the CRA infringed inter alia Article 6, which can be punished with a fine pursuant to Article 83(5) GDPR. The static maximum would amount to €20 million. The dynamic maximum would amount to €120 million (4% of €3 billion). The fine can amount up to €120 million as this dynamic maximum is higher than the static maximum of €20 million. As a consequence, the fine is allowed to exceed the static maximum of €20 million, but must not exceed the applicable legal maximum of €120 million.

Example 8b – Static maximum
A retailer of sunglasses operates an online shop, which allows customers to place their orders. By way of the order form the retailer processes also personal data, including bank account details. The retailer fails to provide for a proper https transport encryption so that third parties are potentially able to intercept the personal data during the transaction. The retailer infringes Article 32(1) GDPR and can be fined pursuant to Article 83(4) GDPR. The retailer's annual worldwide turnover of the preceding year amounts to €450 million. In this case the static maximum of €10 million is higher than the dynamic maximum of €9 million (=2% of €450 million), so that the maximum of €10 million takes precedence. Therefore, the fine must not exceed the legal maximum of €10 million.

Example 8c – Controllers and processors that are not an undertaking
A municipality has an online system that allows its citizens to register for appointments, such as to apply for a passport or a marriage license. The municipality is the sole controller for this online system. Unfortunately, it is found that the system also transmits on a permanent basis the collected data to external servers of a processor in an inadequate third country, where they are stored. No adequate safeguards are put in place with regard to the third country transfer. Except for the transfer, the data are collected and processed on the basis of valid consent. The municipality infringed Article 44 GDPR by transferring special categories of personal data into an inadequate third country without appropriate safeguards. Therefore, it can be fined pursuant to Article 83(5). As the municipality does not meet the definition of an undertaking the static legal maximum applies, so that the fine must not exceed €20 million. However, this is only the case if the Member State in which this municipality is located has not laid down specific rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State (Article 83(7) GDPR).

[43] As for the term "undertaking", please note Chapter 6.2.1 of these Guidelines.
[44] As for the term "turnover", please note Chapter 6.2.2 of these Guidelines.
[45] 2% of 500 million amounts to 10 million (the static maximum amount envisaged in Article 83(4) GDPR) and 4% of 500 million amounts to 20 million (the static maximum amount envisaged in Article 83(5) GDPR).

6.2 - Determining the undertaking's turnover and corporate liability

117. In order to determine the correct turnover for the dynamic legal maximum, it is important to understand the concepts of undertaking and turnover as used in Article 83(4)–(6) GDPR. In this regard, utmost consideration must be given to the recitals of the GDPR, provided by the European legislator for guidance on GDPR interpretation.

6.2.1 - Determining an undertaking and corporate liability

118. As for the term "undertaking", the European legislator provides explicit further clarification. Recital 150 GDPR states: "Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes."

119. Therefore, Article 83(4)–(6) GDPR in light of recital 150 relies on the concept of undertaking in accordance with Articles 101 and 102 TFEU,[46] without prejudice to Article 4(18) GDPR (which gives a definition of an enterprise) and Article 4(19) GDPR (which defines a group of undertakings). The former concept is mainly used in Chapter V GDPR, in the phrase group of enterprises engaged in a joint economic activity. Besides that, the term is applied in a general sense, not as the addressee of a provision or obligation.

120. Accordingly, in cases where the controller or processor is (part of) an undertaking in the sense of Articles 101 and 102 TFEU, the combined turnover of such undertaking as a whole can be used to determine the dynamic upper limit of the fine (see Chapter 6.2.2), and to ensure that the resulting fine is in line with the principles of effectiveness, proportionality and dissuasiveness (Article 83(1) GDPR)[47].

121. The Court of Justice has developed a vast body of case law on the concept of undertaking. The term 'undertaking' "encompasses every entity engaged in an economic activity, regardless of the legal status of the entity and the way in which it is financed."[48] For the purpose of competition law, "undertakings" are therefore identified with economic units rather than legal units. Different companies belonging to the same group can form an economic unit and therefore an undertaking within the meaning of Articles 101 and 102 TFEU[49].

122. In line with settled CJEU case law the term undertaking in Articles 101 and 102 TFEU can refer to a single economic unit (SEU), even if that economic unit consists of several natural or legal persons. Whether several entities form a SEU depends largely on whether the individual entity is free in its decision-making ability or whether a leading entity, namely the parent company, exercises decisive influence over the others. The criteria for determining this are based on the economic, legal and organizational links between the parent company and its subsidiary, for example, the amount of the participation, personnel or organizational ties, instructions and the existence of company contracts[50].

---

[46] As already clarified in WP253 and later confirmed by the EDPB in Endorsement 1/2018 on 25 May 2018. See also EDPB Binding Decision 1/2021, para. 292 and Regional Court Bonn, case 29 OWi 1/20, 11 November 2020, para. 92.

[47] See Binding Decision 1/2021, paras. 412 and 423, and also cases C-286/13 P, *Dole food*, para. 149 and C-189/02 P, *Dansk*, para. 258.

[48] Case C-41/90, *Höfner and Elser v. Macrotron GmbH*, para. 21. See also, for example, joined cases C-159 and 160/91, *Poucet and Pistre v. Assurances Générales de France*, para. 17; case 364/92, *SAT Fluggesellschaft mbH v. Eurocontrol*, para. 18; joined cases C-180-184/98, *Pavlov and Others*, para. 74; and case C-138/11, *Compass-Datenbank GmbH v. Republik Österreich*, para. 35.

[49] case C-516/15 P, *Akzo Nobel and Others v Commission*, para. 48.

[50] See case C-90/09 P, *General Química and Others v Commission*. The main criterion to establish this is 'decisive influence', which should be constructed based on factual evidence (economic, organisational and legal links). Moreover,

123. In line with the SEU doctrine, Article 83(4)–(6) GDPR follow the principle of direct corporate liability, which entails that all acts performed or neglected by natural persons authorized to act on behalf of undertakings are attributable to the latter and are considered as an act and infringement directly committed by the undertaking itself.[51] The fact that certain employees did not comply with a code of conduct is not sufficient to disrupt this attribution[52]. Rather it is only disrupted where the natural person acts solely for its own private purposes or for purposes of a third party, thereby becoming itself a separate controller (i.e. the natural person has acted in excess of their permitted remit)[53]. This European Union law principle and scope of corporate liability takes precedence and must not be undermined by limiting it to the acts of certain functionaries (like principal managers) by contradicting national law. It is not relevant which natural person acted on behalf of which of the entities. The supervisory authority and national courts therefore must not be required to determine or identify a natural person in the investigations or the fining decision[54].

124. In the specific case where a parent company holds 100% of shares or almost 100% of shares in a subsidiary which has infringed Article 83 GDPR and therefore is able to exercise decisive influence over the conduct of its subsidiary, a presumption arises that the parent company does in fact exercise this decisive influence over the conduct of its subsidiary (so-called *Akzo* presumption)[55]. This also applies if the parent company does not directly hold the shares in the total capital directly, but indirectly through one or more subsidiaries[56]. For example, there might also be a chain of subsidiaries, where one entity holds 100% or almost 100% of shares of an intermediate entity that holds 100% or almost 100% of shares of another entity, and so forth. Also a parent company might hold 100% or almost 100% of shares of two entities that each hold about 50% of an entity, thereby providing the parent company with decisive influence on all of them. In those circumstances, it is sufficient for the supervisory authority to prove that the subsidiary is directly or indirectly wholly or almost wholly owned by the parent company in order to presume – as a rule of practical experience – that the parent exercises a decisive influence.

125. However, the *Akzo* presumption is not an absolute one, but can be rebutted by other evidence[57]. In order to rebut the presumption, the company(ies) must provide evidence relating to the organizational, economic and legal links between the subsidiary and its parent company which are apt to demonstrate that they do not constitute a SEU despite holding 100% or almost 100% of shares. In order to ascertain whether a subsidiary itself acts autonomously, account must be taken of all the relevant factors relating to those links that tie the subsidiary to the parent company, which may vary from case to case and cannot therefore be set out in an exhaustive list.

126. If, on the other hand, the parent company does not hold all or almost all of the capital, additional facts must be evidenced by the supervisory authority to justify the existence of a SEU. In such a case, the supervisory

there is a rebuttable presumption of influence in case of a wholly owned subsidiary. See case C-97/08 P, *Akzo* and joined cases C-293/13 and 294/13, *Fresh Del Monte*.

[51] See joined cases C-100 to 103/80, *SA Musique Diffusion française and others v Commission*, para. 97 and case C-338/00 P, *Volkswagen v Commission*, paras. 93 to 98.

[52] Case C-501/11 P, *Schindler Holding and Others v Commission*, para. 114; Therefore, it is important for corporations that their compliance management system is not a mere "paper shield", but actually effective in practice.

[53] See in particular Guidelines 07/2020 on the concepts of controller and processor in the GDPR ("EDPB Guidelines 07/2020"), para 19.

[54] Case C-338/00 P, *Volkswagen v Commission*, para. 97 and 98; any conflicting national legislation is incompliant with the GDPR and the principle of effectiveness and insofar must not be applied.

[55] Case C-97/08 P, *Akzo Nobel and Others v Commission*, paras. 59 and 60.

[56] Cases T-38/05, *Agroexpansión v Commission* and C-508/11 P, *Eni v Commission*, para. 48.

[57] See, among others, case C-595/18 P, *The Goldman Sachs Group v Commission*, ECLI:EU:C:2021:73, para. 32, quoting case C 611/18 P, *Pirelli & C. v Commission*, not published, para. 68, and the case law cited.

authority has to demonstrate, not only that the parent company has the ability to exercise decisive influence over the subsidiary, but also that it has actually exercised such decisive influence so that it can intervene at any time in the subsidiary's freedom of choice and determine its behavior. The nature or type of instruction is irrelevant when determining the parent company's influence.

127. The fine is addressed[58] to the (joint-) controller(s)/processor(s), and the competent supervisory authority has the option to hold the parent company jointly and severally liable[59] for the payment of the fine.

6.2.2 - Determining the turnover

128. Turnover is taken from the annual accounts of an undertaking, which are drawn up with reference to its business year and provide an overview of the past financial year of a company or of a group of companies (consolidated accounts). Turnover is defined as the sum of all goods and services sold. The term turnover within the meaning of Article 83(4)–(5) GDPR is to be understood in terms of the net turnover of Directive 2013/34/EU[60]. According to this directive, net turnover means the amount derived from the sale of products and the provision of services after deducting sales rebates and value added tax (VAT) and other taxes directly linked to turnover.[61]

129. Turnover is taken from the presentation of the profit and loss account within the meaning of Annexes V or VI to Article 13(1) of Directive 2013/34/EU under the heading "net turnover". Net turnover includes revenue from the sale, rental and leasing of products and revenue from the sale of services less sales deductions (e.g. rebates, discounts) and VAT. Revenue therefore does not include items which are unrelated to the business object/sector of the company such as for example the proceeds from the sale of fixed assets, rental of unused parts of buildings, insurance premiums, commissions and interest income in case of an industrial company.[62]

130. If the undertaking is subject to the obligation within the meaning of Article 21 et seq. of Directive 2013/34/EU and has to prepare consolidated annual financial statements, these consolidated financial statements of the parent company heading the group are relevant for reflecting the combined turnover of the undertaking. If such statements do not exist, any other documents shall be obtained and used that are apt to infer the worldwide annual turnover of the undertaking in the relevant business year.

131. Article 83(4)–(6) GDPR state that the total worldwide annual turnover of the preceding financial year is to be used. As to the question of which event the term "preceding" relates to, the CJEU case law in competition law is also to be applied for GDPR fines so that the relevant event is the fining decision issued by the supervisory authority and neither the time of infringement nor the court decision[63]. In case of cross-border processing the relevant fining decision is not the draft decision, but rather the final decision issued by the

[58] The decision is addressed and delivered to the controller(s)/processor(s) as the offender(s) of the infringement and can additionally be addressed and delivered to other legal entities of the SEU that are jointly and severally liable for the fine.
[59] EDPB Binding Decision 1/2021, para. 290.
[60] Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 788/660/EEC (hereinafter "Directive 2013/34/EU").
[61] Article 2(5) of Directive 2013/34/EU.
[62] Conversely, some of these items are relevant and should be included in the revenue in case the company operates for example in the banking sector (commissions and interest income) or in the insurance sector (insurance premiums).
[63] Regional Court Bonn, case 29 OWi 1/20, 11 November 2020, para. 102.

Lead Supervisory Authority[64]. Where the draft decision enters the Article 60 co-decision-making process towards the end of a calendar year, such that the final decision is unlikely to be adopted within that same calendar year, the Lead Supervisory Authority will calculate any proposed fine by reference to the most up to date financial information available as at the date on which the draft decision is circulated to the supervisory authorities concerned for their views. That information will then be updated, as required, prior to the finalization and adoption of the final national decision by the Lead Supervisory Authority.

CHAPTER 7 – EFFECTIVENESS, PROPORTIONALITY AND DISSUASIVENESS

132. It is required that the administrative fine imposed for infringements of the GDPR referred to in Article 83(4)–(6) shall in each individual case be effective, proportionate and dissuasive. In other words, the amount of the fine imposed is tailored to the infringement committed in its specific context. The EDPB considers it incumbent upon the supervisory authorities to verify whether the amount of the fine meets these requirements, or whether further adjustments to the amount are necessary.

133. As explained in Chapter 4, the evaluation performed in this Chapter covers the entirety of the fine imposed and all the circumstances of the case, including e.g. the accumulation of multiple infringements, increases and decreases for aggravating and mitigating circumstances and financial/socio-economic circumstances. It is, however, incumbent upon the supervisory authority to ensure that the same circumstances are not counted twice.

134. In case these adjustments merit an increase in fine, such increase can – by definition – not exceed the legal maximum identified in Chapter 6 above.

7.1 - Effectiveness

135. Generally speaking, a fine can be considered effective if it achieves the objectives with which it was imposed. This could be to reestablish compliance with the rules, to punish unlawful behavior, or both.[65] Moreover, Recital 148 GDPR emphasizes that administrative fines should be imposed "in order to strengthen the enforcement of the rules of this Regulation." The amount of the fine imposed on the basis of these Guidelines should therefore be sufficient to meet these objectives.

136. As Article 83(2) GDPR requires, the supervisory authority has to evaluate the effectiveness of the fine in each individual case. To that end, due regard must be given to the circumstances of the case, and in particular to the assessment made above,[66] bearing in mind that the fine should also be proportionate and dissuasive as outlined below.

7.2 - Proportionality

[64] EDPB Binding Decision 1/2021, para. 298.
[65] Guidelines WP253, p. 6.
[66] As Recital 148 GDPR also outlines: "the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor".

137. The principle of proportionality requires that measures adopted do not exceed the limits of what is appropriate and necessary in order to attain the objectives legitimately pursued by the legislation in question; where 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[67].

138. It follows that fines must not be disproportionate to the aims pursued (i.e. compliance with the rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data), and that the amount of the fine imposed must be proportionate to the infringement, viewed as a whole, account being taken, in particular, of the gravity of the infringement[68].

139. The supervisory authority shall therefore verify that the amount of the fine is **proportionate** both to the severity of the infringement and to the size of the undertaking to which the entity that committed the infringement belongs,[69] and that the fine imposed shall thereby not exceed what is necessary to achieve the objectives pursued by the GDPR.

140. As a particular derivative of the principle of proportionality, the supervisory authority may consider – in accordance with national law – to further reduce the fine on the basis of the principle of inability to pay. Any such reduction requires exceptional circumstances. In line with the European Commission's Guidelines on the method of setting fines[70], there has to be objective evidence that the imposition of the fine would irretrievably jeopardise the economic viability of the undertaking concerned. Furthermore, the risks need to be analysed in a specific social and economic context.

a) **Economic viability:** The undertaking is required to provide detailed financial data (for the last five years as well as projections for the current and next two years) to allow the supervisory authority to examine the likely future development of key factors such as solvency, liquidity and profitability. The European Courts have stated that, the mere circumstance that an undertaking is in a poor financial situation, or will be after a large fine, does not meet the requirement "since recognition of such an obligation would be tantamount to giving an unjustified competitive advantage to undertakings least well adapted to the market conditions."[71] The assessment of the undertaking's ability to pay the fine considers also possible restructuring plans and their state of implementation, relations with external financial partners/institutions such as banks and relations with shareholders[72].

b) **Proof of value loss:** A fine reduction may be granted only if the imposition of the fine would jeopardise the economic viability of an undertaking and cause its assets to lose all or most of their

[67] Case T-704/14, *Marine Harvest*, para. 580, referencing case T-332/09, *Electrabel v Commission*, para. 279.
[68] Ibid.
[69] See, to this effect, case C-387/97, *Commission v Greece*, para. 90, and case C-278/01, *Commission v Spain*, para. 41, in which the fine needed to be "appropriate to the circumstances and proportionate both to the breach that has been established and to the ability to pay of the Member State concerned."
[70] See on this principle, for instance, the Commission Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No 1/2003 (2006/C 210/02).
[71] See joined cases C-189/02 P, C-202/02 P, C-205/02 P to C-208/02 P and C-213/02 P, *Dansk Rørindustri and Others v Commission*, para. 327, citing joined cases 96/82 to 102/82, 104/82, 105/82, 108/82 and 110/82, *IAZ v Commission*, paras. 54 and 55. This was repeated more recently in case C-308/04 P, *SGL Carbon v Commission*, para. 105, and joined cases T-426/10 to T-429/10 and T-438/12 to T-441/12, *Moreda-Riviere Trefilerías and Others v Commission*, paras. 492-493.
[72] See joined cases T-426/10 to T-429/10 and T-438/12 to T-441/12, *Global Steel Wire and Others v Commission*, paras. 521 to 527.

value[73]. A direct causal link between the fine and the significant loss of value of the assets must be shown. There is no automatic acceptance that bankruptcy or insolvency will necessarily result in significant loss of asset value. Furthermore, there can be no question of the fine having threatened the economic viability of an undertaking when that undertaking had itself decided to terminate its activities and to sell all its assets. The undertaking must prove that it will likely exit the market, and its assets will be dismantled or sold at substantially discounted prices with no alternatives for the undertaking (or its assets) to continue operations. This means that the supervisory authority should require the undertaking to prove that there are no clear indications that the undertaking (or its assets) will be acquired another undertaking/owner and continue operations.

c) **Specific social and economic context:** The specific economic context can be considered if the sector concerned is going through a cyclical crisis (e.g. suffering from overcapacity or falling prices) or if companies have difficulties in obtaining access to capital or credit as a result of the prevailing economic conditions. The specific social context is likely to be present in the context of high and/or mounting unemployment at a regional or wider level. It can also be assessed considering the consequences that the payment of the fine may have in terms of increase of unemployment or deterioration of the economic sectors up and downstream[74].

141. If the criteria are met, the supervisory authorities may take the undertaking's inability to pay into account, and reduce the fine accordingly.

7.3 - Dissuasiveness

142. Finally, a dissuasive fine is one that has a genuine deterrent effect[75]. In that respect, a distinction can be made between general deterrence (discouraging others from committing the same infringement in the future) and specific deterrence (discouraging the addressee of the fine from committing the same infringement again)[76]. When imposing a fine, the supervisory authority takes into account both general and specific deterrence.

143. A fine is dissuasive where it prevents an individual from infringing the objectives pursued and rules laid down by Union law. What is decisive in this regard is not only the nature and level of the fine but also the likelihood of it being imposed. Anyone who commits an infringement must fear that the fine will in fact be imposed on them. There is an overlap here between the criterion of dissuasiveness and that of effectiveness[77].

144. The supervisory authorities may consider increasing the fine if they do not consider the amount to be sufficiently dissuasive. In some circumstances, the imposition of a deterrence multiplier can be justified[78]. This multiplier can be set on the discretion of the supervisory authority, in order to reflect the goals of deterrence as outlined above.

[73] See joined cases T-236/01, T-239/01, T-244/01 to T-246/01, T-251/01 and T-252/01, *Tokai Carbon and Others v Commission*, para. 372 and case T-64/02, *Heubach v Commission*, para. 163. See case T-393/10, *Westfälische Drahtindustrie and Others v Commission*, paras. 293-294.
[74] See case C-308/04 P, *SGL Carbon v Commission*, para. 106.
[75] See Opinion of AG Geelhoed in case C-304/02, *Commission v France*, para. 39.
[76] See, inter alia, case C-511/11, *Versalis Spa v Commission*, para. 94.
[77] Opinion of A-G Kokott in joined cases C-387/02, C-391/02 and C-403/02, *Silvio Berlusconi and Others*, para. 89.
[78] See specifically case C-289/04 P, *Showa Denko v Commission*, paras 28-39.

CHAPTER 8 – FLEXIBILITY AND REGULAR EVALUATION

145. The above Chapters outline a general method for the calculation of fines and shall facilitate further harmonization and transparency on the fining practice of supervisory authorities. However, this general method should not be misunderstood as a form of automatic or arithmetical calculation. The individual setting of a fine must always be based on a human assessment of all relevant circumstances of the case and must be effective, proportionate and deterrent with regard to that specific case.

146. It should be kept in mind that these guidelines cannot anticipate each and every possible particularity of a case and in this regard cannot provide an exhaustive guidance for supervisory authorities. Consequently, these guidelines are subject to regular review in order to evaluate whether their application effectively achieves the objectives called for by GDPR. The EDPB may revise these guidelines based on supervisory authorities' further experiences in everyday practical application and may discontinue, change, limit, amend or replace these guidelines at any given time with effect for the future.