Guidelines 04/2026 on the application of the power to impose administrative fines in relation to other corrective powers under the GDPR

Version 1.0

Adopted on 17 September 2026

Version history

Version	Date	Adoption information
version 1.0	17 September 2026	adoption of the guidelines for public consultation

Executive summary

The European Data Protection Board (EDPB) has adopted these guidelines to harmonise the methodology for determining whether an administrative fine should be imposed – in addition to, or instead of, the other corrective measures under Article 58(2) GDPR. Further to administrative fines, the corrective measures include warnings, reprimands, orders, limitations including bans and withdrawal of certification. The supervisory authority should duly consider the purposes of the corrective powers available (which may differ or coincide), in order to determine what measure is appropriate, necessary and proportionate to remedy the shortcoming found and to fully enforce the GDPR. These Guidelines, the Imposition Guidelines, complement the previously adopted Calculation Guidelines, focusing on the methodology for calculating the amount of an administrative fine.

The EDPB has outlined the following methodology, consisting of five steps, for determining whether an administrative fine should be imposed for an infringement of the GDPR. The first steps (1–3) cover the legal preconditions for imposing an administrative fine, whereas the following steps (4–5) concern the assessment of whether to impose an administrative fine (in relation to the other corrective measures under the GDPR).

In the **first step**, the supervisory authority will check that the established infringement can lead to an administrative fine. Since not all infringements of the GDPR are subject to administrative fines, the supervisory authority will need to find support either directly in the GDPR or in national law. The **second step** for the supervisory authority is to establish that the party under investigation can be fined for the infringement in question. Who is liable for an infringement, for example the controller or the processor, depends on who is subject to the provision in breach. In the **third step**, the supervisory authority will assess whether the established infringement has been committed intentionally or negligently, since a culpable infringement is a condition for the imposition of an administrative fine.

Then, in order to assess whether to impose an administrative fine (in addition to, or instead of, the other corrective measures under the GDPR), the factors in Article 83(2)(a)–(k) GDPR shall be taken into account. Furthermore, as follows from Recital 148 GDPR, in a case of a minor infringement, a reprimand may be issued instead of a fine.

Therefore, the **fourth step** is for the supervisory authority to establish whether the aggravating and mitigating factors in Article 83(2) GDPR indicate that the infringement is minor. If this is the case, as a general rule, the supervisory authority will not impose an administrative fine. Conversely, if the infringement is not considered minor, there is a strong presumption to impose an administrative fine. In the **fifth step**, the supervisory authority will assess whether the imposition of an administrative fine would be effective, proportionate and dissuasive in the individual case in accordance with Article 83(1) GDPR. In this assessment, the supervisory authority may consider whether there is reason to deviate from the general practice to impose, or to abstain from imposing, an administrative fine, depending on whether the infringement is considered as minor.

These Guidelines and its methodology will be subject to regular review of the EDPB.

Table of Contents

The European Data Protection Board

Having regard to Article 70 (1)(e) and (k) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter '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,

Has adopted the following Guidelines:

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

1 Introduction

1 Consistent enforcement of the data protection rules is central to a harmonised data protection regime. These Guidelines are intended for use by supervisory authorities to ensure such consistent application and enforcement of the GDPR. They express the EDPB's understanding of Article 83 GDPR (the imposition of administrative fines) and its interplay with Article 58(2) GDPR (corrective powers). The following guidance applies to any controller (Article 4(7) GDPR), processor (Article 4(8) GDPR), monitoring or certification body (Article 41 and 43 GDPR) subject to the specific provisions listed in Article 83(4) to (6) GDPR (hereinafter the 'addressee' of a provision or an obligation of the GDPR)[2].

2 Pursuant 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, and such national law does not prevent it, these Guidelines apply to the possibility of imposing administrative fines with respect to public authorities and bodies.

3 These Guidelines cover cross border cases as well as non-cross border cases. For cross border cases, their methodology is not limited to **Draft Decisions** (Article 60(3) to (6) GDPR), **Revised Draft Decisions** (Article 60(5) GDPR), **Final Decisions** (Article 60(7) to (10) and Article 65(6) GDPR) or **Provisional Measures** (Article 66(1) GDPR), but should also be considered, to the extent appropriate, in the drafting of the (preliminary) identification and (preliminary) reasoning with regards to intended corrective measures in the **Summary of Key Issues** (Article 10(2)(e) Procedural Rules Regulation[3]) as well as the **Preliminary Findings** (Article 19(2) Procedural Rules Regulation).

4 These Guidelines are not exhaustive, and nor will they provide explanations about the differences between administrative, civil or criminal law systems when imposing administrative sanctions in general.

5 Pursuant 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 EDPB shall, in particular, draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58 GDPR and the setting of administrative fines pursuant to Article 83 GDPR.

6 The Article 29 Working Party issued Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679 (WP253) (the 'WP29 Guidelines'), which were endorsed by the EDPB. Later, the EDPB adopted Guidelines 04/2022 on the calculation of administrative fines under the GDPR (the 'Calculation Guidelines'). The aim of the Calculation Guidelines is to harmonise the methodology that supervisory authorities use when calculating the amount of the fine. The Calculation Guidelines complement the WP29 Guidelines, which rather focus on the circumstances in which to impose a fine in relation to other corrective powers, and interpret the criteria of Article 83 GDPR in this respect.

7 Since the entry into force of the GDPR, the supervisory authorities have elaborated practices and gained valuable experience in relation to the imposition of administrative fines under the GDPR. In addition, the Court of Justice of the European Union (CJEU) has made important clarifications regarding, in particular, the calculation and the conditions for imposing an

[2] See also Section 4.2, paragraph 40.
[3] Regulation (EU) 2025/2518 of the European Parliament and of the Council of 26 November 2025 laying down additional procedural rules on the enforcement of Regulation (EU) 2016/679.

administrative fine[4]. Therefore, the EDPB now deems it necessary to give more developed and specific guidance regarding the preconditions for imposing an administrative fine, as well as to provide a methodology for determining whether an administrative fine should be imposed in addition to, or instead of, the other corrective measures under the GDPR. Such guidance is needed to ensure a consistent and harmonised approach among supervisory authorities as regards the imposition of administrative fines and other corrective measures. The supervisory authorities will reflect this common approach in their enforcement in accordance with the local administrative and judicial laws applicable to them.

8 The present guidelines replace the WP29 Guidelines, complement the Calculation Guidelines and can be referred to as the 'Imposition Guidelines'.

2 Overview of the methodology for determining whether to impose an administrative fine

9 Notwithstanding cooperation and consistency duties, the imposition of administrative fines under the GDPR is at the discretion of the supervisory authority. Taking this into account, the EDPB has outlined the following methodology – which consists of five steps – for determining whether an administrative fine should be imposed for an infringement of the GDPR. Step 1–3 cover the legal preconditions for imposing an administrative fine, whereas step 4–5 concern the assessment of whether to impose an administrative fine in relation to the other corrective measures under the GDPR.

Step 1	Can the infringement lead to an administrative fine? **(Section 4.1)**
Step 2	Can the party under investigation be fined for the infringement? **(Section 4.2)**
Step 3	Has the infringement been committed with intent or negligence? **(Section 4.3)**
Step 4	Do the factors in Article 83(2) GDPR indicate a minor infringement? **(Section 5.2)**
Step 5	Would the imposition of an administrative fine be effective, proportionate and dissuasive? **(Section 5.3)**
Step 5 a	The infringement is considered minor – an administrative fine should not be imposed **(Section 5.3.2)**
Step 5 b	The infringement is not considered minor – an administrative fine should be imposed **(Section 5.3.3)**

10 These Guidelines follow a step-by-step approach, though it should be noted that supervisory authorities are not obliged to follow all the steps if they are not applicable in a given case. Nor are they obliged to provide reasoning surrounding aspects of the Guidelines that are not applicable, in particular with respect to the various factors as listed in Article 83(2) GDPR. The factors in Article 83(2) GDPR are used both when deciding whether to impose an administrative fine and when calculating the fine. Therefore, the conclusions reached in the first part of the assessment, namely whether a fine should be imposed, can be used in the

[4] Please refer to Section 4.3 in this regard.

second part concerning the amount of the fine. In this way, a repeated assessment of the same criteria can be avoided.

11 The examples in these Guidelines are illustrations of the effect that circumstances in a specific case may have on the decision of whether to use, and if so which, corrective measures under the GDPR. Atypical examples may also occur due to specific national circumstances. However, the supervisory authorities must perform a full assessment of the relevant factors in each individual case. The consideration of the circumstances in these imaginary cases cannot be considered precedents or indications of how the supervisory authority must reason in real-life cases.

12 Notwithstanding these Guidelines, supervisory authorities remain subject to all procedural obligations under national and EU law, including the duty to state sufficient reasons for their decisions and their obligations under the one stop shop mechanism. The mere reference to these Guidelines cannot replace the reasoning to be provided in a specific case.

13 These Guidelines and its methodology will be subject to regular review of the EDPB.

3 Corrective powers under Article 58(2) GDPR

3.1 Purposes of the corrective powers

14 Administrative fines contribute to the strengthening of the protection of natural persons and are a key element in ensuring respect for their rights and a high level of protection[5]. In order to understand the considerations for imposing administrative fines in an individual case, it is important to take a closer look at the overall enforcement framework and the relationship between the different powers entrusted to the supervisory authorities by the EU legislator.

15 Article 58(2) GDPR provides for various corrective powers, which the supervisory authority may adopt as an appropriate action in order to react to an infringement of the GDPR[6]. In such a situation the supervisory authority must determine – within its discretion – if and which action(s) is or are appropriate and necessary. To that aim, supervisory authorities should take all relevant circumstances of the specific case into consideration[7]. When determining the appropriate and necessary action, the supervisory authority should give due consideration to the respective purposes of the corrective powers. The purposes of the various powers can be deduced by way of interpretation, taking into account the legislative notions as outlined in the recitals of the GDPR.

16 While the term ‘corrective powers’ in a broad sense can be used to refer collectively to all the powers listed in Article 58(2) GDPR to distinguish them from the investigative powers in Article 58(1) GDPR, the wording in the recitals of the GDPR is more distinct. In this regard, the first sentence of Recital 129 GDPR differentiates further between ‘corrective powers’ (in a strict sense) on the one hand and ‘sanctions’ on the other hand. An equivalent distinction is made in Recital 148, where the terms ‘appropriate measures’ on the one hand and ‘penalties’ on the other hand are used. While Recital 129 provides for general remarks and legal principles to

[5] Judgment of the CJEU of 5 December 2023, Deutsche Wohnen, C-807/21, EU:C:2023:950, paragraph 73 (hereinafter C-807/21, Deutsche Wohnen); Judgment of the CJEU of 5 December 2023, Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos, C-683/21, EU:C:2023:949, paragraph 78, (hereinafter: C-683/21, Nacionalinis visuomenės sveikatos centras).

[6] Judgment of the CJEU of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559, paragraph 111 (hereinafter: C-311/18, Facebook Ireland and Schrems); Judgment of the CJEU of 7 December 2023, SCHUFA Holding (Discharge from remaining debts), C-26/22 and C-64/22, EU:C:2023:958, paragraph 57; Judgment of the CJEU of 26 September 2024, Land Hessen, C-768/21, EU:C:2024:785, paragraphs 33, 37 (hereinafter: C-768/21, Land Hessen).

[7] C-311/18, Facebook Ireland and Schrems, paragraph 112; C-768/21, Land Hessen, paragraphs 33, 37.

be observed for all powers without much of a distinction, Recital 148 provides for additional considerations when making a decision with regard to different types of measures. In this regard Recital 148 outlines, that in order to strengthen the enforcement of the rules of the GDPR, 'penalties' including administrative fines should be imposed for any infringement, in addition to, or instead of 'appropriate measures'. Therefore, the legislator indicates that some corrective powers can be used cumulatively, where appropriate, and depending on their purpose.

17 This means that some corrective measures have primarily the purpose of (re-)establishing a (specific) state of compliance (e.g. compliance order) and indirectly also encouraging compliant conduct for the future, while others primarily aim for a specific and general deterrent effect (e.g. administrative fine), as well as to strengthen the enforcement of the rules provided by the GDPR[8]. These different purposes and effects must be taken into account, when deciding if and what measures are appropriate, necessary and proportionate to (1) remedy the shortcoming found and (2) fully enforce the GDPR.

3.2 Administrative fines

18 Administrative fines, as defined in Article 58(2)(i) GDPR, are a central element in the enforcement regime introduced by the GDPR, and are a powerful part of the enforcement toolbox of the supervisory authorities together with the other measures in Article 58 GDPR[9]. However, pursuant to Article 83(1) GDPR, the obligation of each supervisory authority when concluding on the infringed provision is that the imposition of the administrative fine is effective, proportionate and dissuasive. In this context, it is precisely dissuasiveness that indicates an additional or different purpose of administrative fines from that of the other (or most) measures referred to in Article 58(2) GDPR. Therefore, administrative fines clearly have a punitive function and purpose[10].

19 Pursuant to Article 83(2) GDPR, administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, the other corrective measures referred to in Article 58(2) GDPR.

20 The wording of Article 83(2) GDPR might lead to the conclusion that the imposition of an administrative fine is possible in addition to all of the measures listed in Article 58(2) GDPR. However, due regard should be given when combining measures since not all combinations of measures may be appropriate. Stemming from Article 83(2) and Recital 148 GDPR, the supervisory authority has the responsibility to choose the most appropriate (in accordance with the purpose pursued) measure(s). In the cases mentioned in Article 83(4) to (6) GDPR, this choice should be made taking all corrective measures into consideration, including the imposition of an administrative fine, either accompanying another corrective measure under Article 58(2) GDPR or on its own. That interpretation should be supplemented by a teleological

[8] However, only the administrative fine of the GDPR meets the so-called Engel criteria in terms of punitive purpose and severity of a penalty in the broad sense of the European Convention on Human Rights and the Charter of Fundamental Rights and Freedoms of the European Union (see for GDPR fines: AG Emiliou, Opinion of 4 May 2023, C-683/21, Nacionalinis visuomenės sveikatos centras, paragraph 74. See for Engel criteria the following settled case law: European Court of Human Rights, judgment 8 June 1976, Case of Engel and Others VS the Netherlands, application no. 5100/71, 5101/71, 5102/71, 5354/72, 5370/72; judgment of the CJEU of 5 June 2012, Bonda, C-489/10, EU:C:2012:319, paragraphs 36-46; judgment of the CJEU of 26 February 2023, Åkerberg Fransson, C-617/10, EU:C:2013:105, paragraphs 35-36; judgment of the CJEU of 20 March 2018, Menci, C-524/15, EU:C:2018:197, paragraphs 26-33; judgment of the CJEU of 22 March 2022, bpost, C-117/20, EU:C:2022:202, paragraphs 25-26; judgment of the CJEU of 4 May 2023, MV, C-97/21, EU:C:2023:371, paragraphs 38-48; judgment of the CJEU of 14 September 2023, Volkswagen Group Italia, C-27/22, EU:C:2023:663, paragraph 48-55.

[9] Note that the legal systems of Denmark and Estonia do not allow for administrative fines as set out in the GDPR. See Recital 151 GDPR.

[10] Judgment of the CJEU of 21 December 2023, Krankenversicherung Nordrhein, C-667/21, EU:C:2023:1022, paragraph 85 (hereinafter: C-667/21, Krankenversicherung Nordrhein).

interpretation based on the purpose of the imposition of each of the measures listed below. For example, in the case of the imposition of a warning as a corrective measure, an administrative fine cannot be imposed, since an infringement of the provisions of the GDPR has not yet occurred.

3.3 Warnings

21 Pursuant to Article 58(2)(a) GDPR, a supervisory authority may issue a warning to a controller or processor if the intended processing operations (i.e. processing operations that have not yet taken place) are likely to infringe the provisions of the GDPR. The wording of Article 58(2)(a) GDPR clearly states that a warning is a power to be exercised ex ante, when an infringement of a provision of the GDPR has not yet occurred but is likely to happen if the controller or the processor puts the intended processing operations into practice. For example, a warning could be issued in case of a prior consultation pursuant to Article 36 GDPR, where a supervisory authority is of the opinion that the intended processing would infringe the GDPR, in particular where the controller has insufficiently identified or mitigated the risk.

22 As part of the corrective measures of Article 58(2) GDPR, a warning has a specific purpose that can be qualified as preventive. On that basis, and in view of the fact that the purpose of the warning is to warn the controller or processor that its actions are likely to infringe the GDPR, a warning has a special place which excludes the application of all other corrective measures, including administrative fines.

23 Therefore, in cases where a warning pursuant to Article 58(2)(a) GDPR could be imposed, i.e. when processing operations are likely to infringe provisions of the GDPR, an infringement of the GDPR has not yet occurred. Therefore, an administrative fine cannot be imposed in addition to a warning for the same conduct. This is due to the fact that a precondition for imposing a fine is that the supervisory authority has established that the controller or processor has committed an infringement referred to in Article 83(4) to (6) GDPR. The same applies to measures which are primarily intended to restore the legal situation. Indeed, the mere finding that certain processing operations might infringe the GDPR implicitly means that the supervisory authority has not yet conducted an investigation or established, with a high degree of probability, an infringement on the basis of established facts. The unlawful processing has not yet taken place, so the imposition of any other corrective measure, in addition to the warning, would be incompatible with Article 58(2) GDPR. However, there is nothing to prevent the supervisory authority from issuing a warning and another corrective measure for separate conducts within the same decision.

Example 1: Intended implementation of AI system for analysing employee communication and emotion

A controller informs the supervisory authority of the intention to implement an AI system that analyses employees' electronic communication (emails, calendars, time recording at meetings etc.) for the purpose of assessing their productivity. Pursuant to Article 58(2)(a) GDPR the supervisory authority issues a warning as the intended processing lacks a legal basis, a proper data protection impact assessment (DPIA) and would most likely infringe Article 22 GDPR (automated decision-making). Despite the issued warning, the controller introduces the system. Additionally, the controller intends to implement a system for emotional analysis of employees based on facial expression during videoconferencing, tone of voice and speech patterns for reducing so-called ‘emotional exhaustion’. In this case, a supervisory

authority could issue an administrative fine for the unlawful implementation of an AI system assessing the productivity, and issue a warning for the intended emotional analysis.

24 Where the controller proceeds with the processing operations despite a warning, a previous warning speaks for the infringement being intentional[11]. However, in the assessment of whether to impose an administrative fine under Article 83(2) GDPR, a failure to comply with the warning cannot be taken into account as a relevant previous infringement by the controller or processor[12]. Failure to comply with a previous warning may, however, be considered as non-compliance with a measure previously ordered against the controller or processor with regard to the same subject matter[13].

3.4 Reprimands

25 Pursuant to Article 58(2)(b) GDPR, each supervisory authority has the power to issue reprimands to a controller or processor where processing operations have infringed the GDPR. Recital 148 GDPR states that in order to strengthen the enforcement of the GDPR, penalties, including administrative fines, should be imposed for any infringement, in addition to, or instead of appropriate measures imposed by the supervisory authority. Deriving from the specific wording of that Recital ('penalties, including administrative fines'), in addition to administrative fines, the GDPR provides for other kinds of measures with a deterrent effect (e.g. a reprimand) and therefore also distinguishes between corrective measures with different purposes. This means that it is not necessary to issue both a fine and a reprimand for the same infringement, considering the alternate nature stemming from the second sentence of Recital 148 GDPR ('instead') as well as the common purpose of both measures (deterrence). It should, however, be noted that Article 58(2)(i) and Article 83(2) GDPR do not in principle exclude the combination of a fine and a reprimand (or other corrective measures), depending on the circumstances in a specific case.

26 Pursuant to Recital 148 GDPR, a reprimand may be issued instead of a fine in a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person. However, it is generally, but not necessarily only, in these two cases that a reprimand can be issued against a controller or processor. The GDPR leaves the supervisory authority discretion as to the manner in which it must remedy the shortcoming found and ensure that the GDPR is fully enforced. Further to the cases referred to in Recital 148 GDPR, for example, a supervisory authority may decide to issue a reprimand where the fine would constitute a disproportionate burden to a legal person (instead of a natural person, as provided for by Recital 148 GDPR). Furthermore, in Member States where national legislation does not allow for the imposition of administrative fines in relation to public authorities, a reprimand (or other measures established by national law) may be issued instead of a fine. Finally, the wording 'may' in Recital 148 GDPR implies that even in these particular cases a supervisory authority has a discretionary power to issue a reprimand or an administrative fine.

3.5 Orders

27 As indicated above[14], the following corrective measures referred to in Article 58(2) GDPR are part of a set of measures which, in terms of their content and purpose, are intended to remedy

[11] See Article 83(2)(b) GDPR.
[12] See Article 83(2)(e) GDPR.
[13] See Article 83(2)(i) GDPR.
[14] See Section 3.1.

an infringement of the GDPR by requiring the controller or processor to bring specific processing operations into compliance with relevant provisions.

28 These measures are:

- to order the controller or processor to comply with the data subject's requests to exercise their rights Article 58(2)(c) GDPR),
- to order the controller or processor to bring processing operations into compliance, where appropriate, in a specified manner and within a specified period (Article 58(2)(d) GDPR),
- to order the controller to communicate a personal data breach to the data subject (Article 58(2)(e) GDPR),
- to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 GDPR and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 18 GDPR (Article 58(2)(g) GDPR),
- to order the suspension of data flows to a recipient in a third country or to an international organisation (Article 58(2)(j) GDPR).

29 The supervisory authority uses these corrective powers in the event of a finding of non-compliance of a specific act or failure to act of the addressee of a provision, as these measures are intended to ensure compliance with the GDPR, and indirectly also encourage compliant conduct for the future. Depending on the circumstances of each case, the supervisory authority will apply the most appropriate, effective and proportionate measures. In view of the content of the individual measures, it is clear that not all the orders referred to in paragraph 28 will be considered as appropriate measures for certain infringements of the GDPR, but only those closely linked to the content of the infringement. For example, in the event of a finding of an infringement of Article 34(1) GDPR (Communication of a personal data breach to the data subject), the supervisory authority could order the controller to communicate the personal data breach to the data subject as this measure may be considered to be the most appropriate one to remedy the shortcoming found. Another example would be to order the suspension of data flows for the infringement of Articles 44 to 49 GDPR (Transfers of personal data to third countries or international organisations). An order of suspension of transfer of personal data could be ordered with a view to protecting the rights and freedoms of natural persons for a limited period of time, until the conditions for lawful transfer under Chapter V GDPR are fulfilled. As long as these conditions are not fulfilled, the order of suspension would remain.

30 Since those measures are intended to remedy the shortcoming found, there is nothing to prevent the supervisory authority from imposing a measure with deterrent effect in addition to those measures, in accordance with the provisions of the GDPR. Even in the case where an administrative fine is not accompanied by an order, there is still an obligation to bring the processing into compliance with the GDPR.

3.6 Limitations, including bans

31 In accordance with Article 58(2)(f) GDPR, supervisory authorities may also impose a temporary or definitive limitation including a ban on processing addressed to the controller or processor. This measure allows for the temporary or permanent restriction or prohibition of the processing of personal data.

32 The interim measure is intended to regulate the protection of personal data in a time-limited manner, namely, until the facts have been clarified to the extent that it is possible to establish either the compliance of the conduct or that the conditions for lawful processing are not met.

An interim measure is conditional on the need to provisionally protect the rights of data subjects, as otherwise they may suffer consequences which are difficult to remedy. The imposition of an interim measure may be followed by the imposition of another more extensive permanent measure.

33 Contrary to an interim measure, a permanent or definitive measure is always subject to a prior finding of unlawful processing. A supervisory authority could first impose a temporary limitation of processing and after the conclusion of the investigation procedure, also impose a permanent limitation or ban on processing. The permanent measure in question, in terms of restriction of processing or prohibition of processing, may also follow other corrective measures where such measures cannot restore the legal situation and protect the rights of data subjects.

34 As a rule, an administrative fine can be imposed in addition to a limitation or ban pursuant to Article 58(2)(f) GDPR. However, where a limitation or ban refers to a situation where an infringement of the GDPR has not yet been established (e.g. future processing), an administrative fine cannot be imposed in addition to such a measure for the same conduct[15].

3.7 Withdrawal of certification

35 Pursuant to Article 58(2)(h) GDPR, the supervisory authorities have the power to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 GDPR, or to order the certification body not to issue certification if the requirements for the certification are not, or are no longer, met. This is, in essence, a repetition of the supervisory authority's already established power under Article 42(7) GDPR to withdraw the certificate itself and, as a corrective measure, to order the certification body to do so. Under Article 42(7) GDPR the power to withdraw the certificate is given to both the supervisory authority and the certification body. Therefore, the supervisory authority would not necessarily have to withdraw the certificate itself if it finds that there are grounds for doing so, as it can order the certification body to do so. A measure requiring the certification body to withdraw the certificate would however only be justified due to the specific circumstances of the case, for example if the withdrawal would be carried out more quickly by the certification body. The protection of the rights of individuals could be a reason for such a decision of the supervisory authority.

36 The supervisory authority will have to establish the facts prior to the withdrawal of the certification (either directly or through the certification body). In this context, it will have to establish an infringement of the provisions of the GDPR. It may also impose any other corrective measure, in addition to the measure of withdrawal of the certificate, including the imposition of an administrative fine (or reprimand).

4 Legal preconditions for imposing an administrative fine

4.1 Step 1: Can the infringement lead to an administrative fine?

[15] Cf. the reasoning above in paragraph 23 regarding warnings.

37 The first step of the supervisory authority is to establish that an infringement has occurred. Once verified, it should be confirmed whether the infringement can lead to an administrative fine. This means determining whether there is support for imposing an administrative fine for the infringement directly in the GDPR or in national law. Infringements which have direct support in the GDPR for imposing administrative fines are listed in Article 83(4) to (6) GDPR, which also includes some obligations adopted under national law[16].

38 Although Article 83(4) to (6) GDPR refers to almost all obligations of controllers and processors under the GDPR, it notably does not include Article 10 or Article 24 GDPR. Some Member States have adopted national legislation to allow for imposing administrative fines for infringements of Article 10 and Article 24 GDPR. Article 24 GDPR lays down a general obligation for controllers to implement appropriate technical and organisational measures to ensure that processing is performed in accordance with the GDPR. This provision also requires controllers to be able to demonstrate this[17]. However, since Article 24 GDPR gives expression to the principle of accountability of the controller set out in Article 5(2) GDPR[18], which in turn is listed in Article 83(5) GDPR, an infringement of Article 24 GDPR may amount to an infringement of Article 5(2) GDPR[19].

39 If there is support for imposing an administrative fine for the established infringement, the supervisory authority will move on to step 2 (Section 4.2).

4.2 Step 2: Can the party under investigation be fined for the infringement?

40 The next step for the supervisory authority is to establish that the party under investigation can be fined for the infringement in question. Article 83(4) to (6) GDPR allows for the imposition of administrative fines for the infringement of certain provisions of the GDPR. In order to establish who is liable for an infringement, it is necessary to establish who is the addressee[20] of the specific provision. Depending on the provision, this could be a controller (Article 4(7) GDPR), processor (Article 4(8) GDPR), certification (Article 43 GDPR) or monitoring body (Article 41 GDPR), irrespective of their legal form or status, whether they are a natural or legal person, public authority, agency or other body.

41 These addressees are directly liable not only for infringements committed by their representatives, directors or managers, but also by any other person acting in the course of their business and on their behalf (principle of direct corporate liability)[21]. It is not necessary for there to have been action by, or even knowledge on the part of, the management body[22]. Furthermore, it is not necessary for this liability that the infringement is attributed or attributable to an identified natural person[23]. The fact that employees did not comply with instructions or a code of conduct is not necessarily sufficient to disrupt this liability[24]. Rather it is only disrupted

[16] That is any obligation pursuant to Member State law adopted under Chapter IX as provided for by Article 83(5)(d) GDPR.
[17] Judgment of the CJEU of 14 December 2023, Natsionalna agentsia za prihodite, C-340/21, EU:C:2023:986, paragraph 24 (hereinafter: C-340/21, Natsionalna agentsia za prihodite).
[18] C-340/21, Natsionalna agentsia za prihodite, operative part 3.
[19] With regard to the question of speciality and the relationship between the principles in Article 5 and the more concrete other obligations of the GDPR, see Calculation Guidelines, paragraph 35.
[20] See definition of “addressee” of a provision or an obligation of the GDPR in paragraph 1 above.
[21] C-807/21, Deutsche Wohnen, paragraph 44.
[22] C-807/21, Deutsche Wohnen, paragraph 77; C-683/21, Nacionalinis visuomenės sveikatos centras, paragraph 82.
[23] C-807/21, Deutsche Wohnen, paragraphs 46, 51.
[24] Judgment of the CJEU of 11 April 2024, juris GmbH, C-741/21, EU:C:2024:288, paragraph 51.

where it can be demonstrated that such a person acted solely for its own private purposes or for purposes of a third party, thereby becoming itself a separate controller[25].

42 Persons acting on behalf of a potential addressee are not limited to employees, but also include external natural persons or legal entities, as long as they are acting in the course of their business and on their behalf. Therefore, a controller is also liable for infringements committed by a processor in a situation where the processing of personal data is carried out by a processor on behalf of that controller[26]. Such an attribution to the controller is only disrupted in situations where the processor has processed personal data for its own purposes or where that processor has processed this data in a manner incompatible with the framework of, or detailed arrangements for, the processing as determined by the controller, or in such a manner that it cannot reasonably be considered that that controller consented to this processing[27]. In such cases the processor itself becomes a separate controller for the action that cannot be attributed to the original controller, in accordance with Article 28(10) GDPR. This is irrespective of cases where the processor is directly liable for infringing provisions that are specifically addressed to processors (e.g. Article 28 and 32 GDPR).

43 Even where the attribution of an infringement is disrupted, the original entity can still be separately liable. For instance, a controller can still be held liable for an infringement of Article 32 GDPR, i.e. if they have not implemented any, or insufficient, technical and organisational measures, to adequately combat the risk of such rogue actions of persons that act on their behalf.

44 This liability concept of the GDPR is directly applicable. The conditions for imposing an administrative fine are exhaustive and the GDPR does not leave any margin of discretion to Member States to introduce further procedural or substantive conditions[28]. Article 58(2)(i) and Article 83(1) to (6) GDPR preclude any such national legislation[29].

45 However, the GDPR does not exclude additional national legislation that extends liability for the payment of an administrative fine in order to close potential loopholes in terms of collecting the debt, in line with the principle of practical effectivity. Such national legislation may include e.g. provisions on contingent liability, liability of a legal or economic successor or liability of the parent company, e.g. under national administrative or company law.

46 After having established that the party under investigation can be fined for the infringement in question, the supervisory authority will move on to step 3 (Section 4.3).

4.3 Step 3: Has the infringement been committed with intent or negligence?

47 The next step for the supervisory authority is to assess whether the established infringement has been committed intentionally or negligently. Article 83(4) to (6) GDPR require an infringement of certain provisions of the GDPR for an administrative fine to be imposed. These provisions establish prohibitions or obligations. These provisions are infringed, if there is an objective state of non-compliance with regard to these prohibitions or obligations. Article 83(4)

[25] Calculation Guidelines, paragraph 123, referring to EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, paragraph 19.
[26] C-683/21, Nacionalinis visuomenės sveikatos centras, paragraph 84.
[27] C-683/21, Nacionalinis visuomenės sveikatos centras, paragraph 85.
[28] C-807/21, Deutsche Wohnen, paragraphs 45, 48; C-683/21, Nacionalinis visuomenės sveikatos centras, paragraphs 67, 70.
[29] C-807/21, Deutsche Wohnen, paragraph 60; C-683/21, Nacionalinis visuomenės sveikatos centras, paragraph 61.

to (6) GDPR do not expressly state any additional element, such as negligence or intent,[30] and are insofar limited to the elements as outlined by the referenced GDPR provisions.

48 However, Article 83(2)(b) and Article 83(3) GDPR presume that, when imposing a fine, there is either a situation of negligence or intent[31]. No provision indicates a situation of imposing a fine in the absence of any wrongful conduct[32]. Therefore, it can be deduced that there is another unwritten condition of culpability outside the elements in Article 83(4) to (6) GDPR. Accordingly, Article 83 GDPR does not allow an administrative fine to be imposed, without it being established that the infringement was committed intentionally or negligently by the addressee and that, consequently, a culpable infringement constitutes a condition for such a fine to be imposed[33]. The relevant elements of negligence or intent can be indicated and deduced on the basis of objective elements of conduct gathered from the facts of the individual case[34].

49 'Negligence' requires an awareness component, but not a will component[35]. The GDPR does not require a specific degree of negligence as a requirement to impose an administrative fine. The awareness component is fulfilled, where the addressee of a provision could not be unaware of the infringing nature of their conduct, regardless whether or not they are aware that they are infringing the provisions of the GDPR[36]. The fact that the addressee of a provision has characterised wrongly in law their conduct upon which the finding of the infringement is based cannot exempt them from imposition of an administrative fine, insofar as they could not be unaware of the wrongful nature of their conduct[37]. The decisive factor is whether the addressee of a provision was **in a position** to know that their conduct was unlawful, not whether they actually recognised this[38]. It is therefore not necessary that they have positive knowledge or actual awareness, but rather that they should have known and should have been aware. They are expected to inform and familiarise themselves with the law and its obligations applicable to them as a matter of due diligence. As emphasised by AG Emiliou, the threshold for the element of negligence is so low that it is difficult to envisage situations where the element is not satisfied[39]. The low threshold for the element of negligence has also been confirmed by national courts of appeal[40].

[30] C-807/21, Deutsche Wohnen, paragraph 62.
[31] C-807/21, Deutsche Wohnen, 66-68; C-683/21, Nacionalinis visuomenės sveikatos centras, paragraphs 71-73.
[32] C-807/21, Deutsche Wohnen, paragraphs 66, 68, 74; C-683/21, Nacionalinis visuomenės sveikatos centras, paragraphs 67, 70, 79.
[33] C-807/21, Deutsche Wohnen, paragraph 75; C-683/21, Nacionalinis visuomenės sveikatos centras, paragraphs 67, 80.
[34] Calculation Guidelines, paragraph 56; EDPB 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, adopted on 28 July 2021 (hereinafter: EDPB Binding Decision 1/2021), paragraph 378, EDPB Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR, adopted on 28 July 2022 (hereinafter: EDPB Binding Decision 2/2022), paragraphs 199, 203 and EDPB Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service, adopted on 5 December 2022, paragraph 419 (hereinafter: EDPB Binding Decision 4/2022).
[35] EDPB Binding Decision 1/2021, paragraph 378, EDPB Binding Decision 2/2022, paragraph 199, EDPB Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook Service (Art. 65 GDPR) (hereinafter: EDPB Binding Decision 3/2022), paragraph 450 and EDPB Binding Decision 4/2022, paragraph 419.
[36] C-807/21, Deutsche Wohnen, paragraph 76; C-683/21, Nacionalinis visuomenės sveikatos centras, paragraph 81; by analogy: judgments of the CJEU of 18 June 2013, Schenker & Co. and Others, C-681/11, EU:C:2013:404, paragraph 37 (hereinafter: C-681/11, Schenker & Co. and Others) and the case-law cited; judgment of the CJEU of 25 March 2021, Lundbeck v Commission, C-591/16 P, EU:C:2021:243, paragraph 156 (hereinafter: C-591/16 P, Lundbeck v Commission); judgment of the CJEU of 25 March 2021, Arrow Group and Arrow Generics v Commission, C-601/16 P, EU:C:2021:244, paragraph 97 (hereinafter: C-601/16 P, Arrow Group and Arrow Generics v Commission).
[37] By analogy, C-681/11, Schenker & Co. and Others, paragraph 38; C-591/16 P, Lundbeck v Commission, paragraph 157; C-601/16 P, Arrow Group and Arrow Generics v Commission, paragraph 98.
[38] By analogy, C-591/16 P, Lundbeck v Commission, paragraph 158.
[39] AG Emiliou, Opinion of 4 May 2023, C-683/21, Nacionalinis visuomenės sveikatos centras, paragraph 80.
[40] See e.g. the Swedish Administrative Court of Appeal in Stockholm, judgment of 11 March 2023 case no 2828-23 and judgment of 3 June 2025 case no 4512-24, where the court states that the company is responsible for its processing activities, including

50 This element may only be absent, where an error in law can be considered as having been unavoidable. Therefore, AG Emiliou has concluded, that in general, 'plain and simple human error' may be indicative of negligence and points out that mere doubts about the legality may already constitute acceptance of potentially infringing the GDPR and be considered gross negligence[41]. Therefore, good faith can only be invoked in very exceptional circumstances, where an error could not have been reasonably overcome through the exercise of due diligence. As highlighted by AG Kokott, such an 'unavoidable error' in law occurs only very rarely and may exist only where the addressee of a provision took all possible and reasonable steps to avoid the alleged infringement[42]. Where the law leaves room for interpretation, the absence of legal literature or EDPB Guidelines does not per se make an error unavoidable. However, where EDPB Guidelines exist, an error is always to be considered avoidable and therefore at least negligent[43].

Example 2: Negligence despite changed legislation

An insurance company transmits personal data of insured persons without a legal basis. The personal data are transmitted to experts commissioned by the company in order to have them examine the medically relevant preliminary questions for the existence of an obligation to pay benefits. When the supervisory authority announces its intention to impose an administrative fine, the company argues that it did not act negligently. Before the GDPR came into force, it was in line with national legal understanding that no legal basis was required for the transfer of data to commissioned experts. The supervisory authority did not inform the company of the change in the law and did not issue a public statement on this issue before it took action against the company. The arguments put forward by the company do not negate the negligence of its actions. When reading the GDPR it is clear that each processing would require a legal basis. The company was in a position to take note of the change in the law and to draw the appropriate legal conclusions from it, but it did not do so. This leads to a finding of negligence with regard to its conduct.

Example 3: Negligence despite missing subjective element to violate the law

A one-person company ignores access requests from data subjects, unaware of its obligation to provide information about the personal data it processes in accordance with Article 15 GDPR. It also objects to the supervisory authority's intention to impose an administrative fine, arguing that it was simply unaware of the obligation and did not intend to violate the law. The owner of the company claims that as a one-person company that actually operates in a completely different field, not related to data protection, it cannot be accused of negligence with regard to the subjective intention to violate the law.

that personal data are processed in line with applicable laws, and since the requirements of the GDPR have not been met, the company could not be unaware of the infringing nature of its conduct.

[41] AG Emiliou, Opinion of 4 May 2023, C-683/21, Nacionalinis visuomenės sveikatos centras, paragraph 81.

[42] AG Kokott, Opinion of 28 March 2013, C-681/11, Schenker & Co. and Others, paragraph 46.

[43] Cf. EDPB Binding Decision 3/2022, paragraph 461, and EDPB Binding Decision 4/2022, paragraph 430.

The intention to violate the law is not necessary for the existence of negligence. The only decisive factor is whether the controller had the opportunity to become aware of the obligation, which is the case here.

Example 4: **a) Negligence despite contrary external legal advice**

A publicly traded company processes the personal data of data subjects in violation of data protection law. It justifies its actions with a legal opinion from a lawyer it has commissioned. The opinion, which opposes the view of the majority of the legal literature, concludes that the company's actions are permissible under data protection law. The company is of the opinion that it cannot be accused of negligence in view of the contrary legal opinion. However, the lawyer's opinion cannot exculpate the company. On the contrary, as the opinion also includes references to e.g. the opposing opinion of the legal literature, the company was aware that its actions could be contrary to the GDPR and was, therefore, in a position of negligence.

b) Negligence despite contrary internal legal advice

The processing of personal data of data subjects by a company violates data protection law. The controller objects to the administrative fine with the argument that a legal assessment conducted by an internal team came to the conclusion that the processing was lawful. However, the internal advice opposed the known opinion of the supervisory authority. The internal legal assessment cannot exculpate the company. This is because the company could have been aware of the supervisory authority's legal opinion and, therefore, also aware that the processing could infringe the GDPR. Therefore, this act constitutes negligence.

c) Trusting external advice blindly

A company does not provide all the information required under Article 13(1) GDPR at the time of collection from the data subjects. It justifies its actions to the supervisory authority by stating that it sought external legal advice, according to which the information provided is legally compliant. When requested by the supervisory authority the company is unable to provide the documentation regarding the alleged consultation and its content.

Since the authority, in the absence of documentation, cannot form a picture of the alleged consultation and is therefore unable to verify whether the external advice was provided on the basis of complete factual information and with knowledge of conflicting views in practice or the literature, the company's argument cannot have any exculpatory effect.

Even if documentation had been available, external advice must not be blindly trusted. There is a wealth of information available from the EDPB and the supervisory authorities regarding the scope of information to be provided

during data collection. Controllers also have a duty to familiarise themselves with the relevant data protection provisions prior to processing of personal data. In this context, the clear wording of Article 13(1) GDPR should have already alerted the controller to the fact that the information it intended to provide was insufficient. Therefore, in this case, it cannot be assumed that there was an unavoidable error in law, and the company acted at least negligently.

51 In contrast to negligence, 'intent' requires two cumulative and distinct components to be fulfilled: a knowledge component and a will component[44]. Having knowledge of a specific matter does not necessarily imply having the 'will' to reach a specific outcome[45].

52 For the requirement to impose a fine it is not necessary to differentiate whether an infringement was intentional or negligent. It is sufficient to establish, that it was 'at least negligent'. However, the degree of culpability may play a role when weighing all factors of the individual case in the step of discretion (see Section 5.2.2).

53 If the established infringement has been committed intentionally or negligently, the supervisory authority will move on to step 4 (Section 5.2).

5 Determining whether an administrative fine should be imposed

5.1 Methodology to determine whether to impose an administrative fine

54 If the supervisory authority finds that the legal preconditions to impose an administrative fine for an infringement are fulfilled (see step 1–3 above), it then needs to assess whether an administrative fine should be imposed (in addition to, or instead of, the other corrective measures under the GDPR).

55 Pursuant to Article 83(2) GDPR, when deciding whether to impose an administrative fine in each individual case the factors in Article 83(2)(a) to (k) GDPR shall be taken into account[46]. These factors characterise either the past or present behaviour of the controller/processor or the infringement itself. The factors in Article 83(2)(a) to (k) GDPR therefore serve to ensure that each infringement is assessed on the basis of all the relevant individual circumstances and that the objectives pursued by the system of penalties provided for in the GDPR are achieved[47].

56 Recital 148 GDPR introduces the concept of 'minor infringement'. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. As provided for by this Recital, when assessing whether the infringement is minor, due regard should be given to the aggravating and mitigating factors as listed in Article 83(2) GDPR[48]. These factors are further

[44] EDPB Binding Decision 1/2021, paragraph 378, EDPB Binding Decision 2/2022, paragraphs 199, 203, EDPB Binding Decision 3/2022, paragraph 450, 454 and EDPB Binding Decision 4/2022, paragraph 419, 423.
[45] EDPB Binding Decision 2/2022, paragraph 203, EDPB Binding Decision 3/2022, paragraph 454 and EDPB Binding Decision 4/2022, paragraph 423.
[46] In this regard, see also paragraph 10.
[47] Judgment of the CJEU of 13 February 2025, ILVA, C-383/23, EU:C:2025:84, paragraph 28 (hereinafter: C-383/23, ILVA).
[48] Such as 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

described in Sections 5.2.1–5.2.11 below. When assessing the criteria in Article 83(2) GDPR, the supervisory authority may, for example, conclude that in the specific circumstances of the case, the infringement is 'minor' since it does not pose a significant risk to the rights of the data subjects concerned and does not affect the essence of the obligation in question. The consequence of an infringement being considered minor is therefore that, as a general rule, an administrative fine should not be imposed, and a reprimand may be imposed instead.

57 Therefore, in order to determine whether an administrative fine should be imposed, the supervisory authority first needs to establish whether the factors in Article 83(2) GDPR indicate that the infringement is minor (step 4). As mentioned, if the infringement is considered minor, as a general rule, the supervisory authority will not impose an administrative fine. Conversely, if the infringement is not considered minor, there is a strong presumption to impose an administrative fine.

58 After having determined whether the established infringement is considered as minor, the supervisory authority will move on to step 5 (Section 5.3). In this step, the supervisory authority will assess whether the imposition of an administrative fine would be effective, proportionate and dissuasive in the individual case. In this assessment, the supervisory authority may consider whether there is reason to deviate from the general practice to impose, or to abstain from imposing, an administrative fine, depending on whether the established infringement is considered as minor (step 5 a/step 5 b). In step 5, the supervisory authority should have due regard to Section 5.3.1 concerning the three overarching criteria for the imposition of administrative fines, namely effectiveness, proportionality and dissuasiveness.

5.2 Step 4: Do the factors in Article 83(2) GDPR indicate a minor infringement?

5.2.1 Introduction

59 Almost all of the obligations of the controllers and processors pursuant to the GDPR are categorised according to their nature in the provisions of Article 83(4) to (6) GDPR. The classification of these obligations only provides an abstract sense of the seriousness of the infringement, as provided for by the EU legislator. Infringements of the core principles of the GDPR, frequently found in Article 83(5) and (6) GDPR, are subject to a higher tier of fine. However, in order to determine whether an infringement can be considered minor the supervisory authority should assess the facts of the case in light of the general criteria provided in Article 83(2) GDPR. By giving due regard to all applicable factors, it may decide based on the facts of a particular case that there is a higher or a more reduced need to react with an administrative fine.

60 Due to national procedural rules, the assessment of the sanction to be applied may be done separately, after the assessment of whether there has been an infringement. For cross border cases, this may therefore limit the amount of detail in a draft decision issued by the lead supervisory authority in those Member States.

61 Given that the factors mentioned in Article 83(2) GDPR are used both when deciding whether to impose an administrative fine and when calculating it, there is some overlap with the Calculation Guidelines in sections 5.2.2–5.2.12 below. It should be noted though that – as explained above in Section 3.1 – the assessment following these guidelines pursue a different purpose, namely whether the factors in Article 83(2) GDPR indicate a minor infringement, and

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.

to determine whether to impose an administrative fine, or another corrective measure. The factors mentioned in Article 83(2) GDPR that have already been explained in the Calculation Guidelines have been incorporated in these guidelines and adapted to the specific context of this assessment where necessary.

5.2.2 Article 83(2)(a) – Nature, gravity and duration of the infringement

62 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 enable the supervisory authority to differentiate it from other infringements of the same kind. This assessment should therefore consider the following specific factors, based on the individual circumstances of the case:

63 The **nature of the infringement**, is assessed going beyond the abstract classification of Article 83(4) to (6) GDPR. In order to analyse the nature of the infringement, 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.

64 The **gravity of the infringement**, as stated in Article 83(2)(a) GDPR, concerns the nature of the processing, but the 'scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them', will also be indicative of the gravity of the infringement.

65 The **nature of the processing**, which includes 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. When the nature of the 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, the supervisory authority may consider to attribute more weight to this factor, depending on the context of the processing and the role of the controller or the processor. 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.

66 The **scope of the processing**, is assessed by 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 processing increases. The larger the scope of the processing, the more weight the supervisory authority may attribute to this factor.

67 The **purpose of the processing,** is assessed taking into consideration whether the processing of personal data falls within the 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 activities 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).

68 The **number of data subjects** concretely but also potentially affected is a further factor to be assessed. 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 proportions 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 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.

69 The **level of damage** suffered and the extent to which the conduct may affect individual rights and freedoms is a further element to be assessed. The reference to the *level* of damage suffered is therefore 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 limited). 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, can be limited to what is functionally necessary to achieve a correct evaluation of the level of seriousness of the infringement as indicated in paragraph 60 of the Calculation Guidelines, without overlapping with the activities of judicial authorities tasked with ascertaining the different forms of individual harm.

70 The **duration of the infringement**. A supervisory authority may generally attribute more weight to an infringement with longer duration. The longer the duration of the infringement, the more likely it is that the infringement is not considered as minor and that an administrative fine will be imposed.

5.2.3 Article 83(2)(b) – Intentional or negligent character of the infringement

71 The GDPR does not require a specific degree of intent or negligence (see Section 4.3). However, the higher the degree of culpability the greater the weight towards (i) not considering the infringement as minor and (ii) a decision to impose an administrative fine. This is particularly true for infringements committed intentionally.

72 In a case of a negligent infringement, different degrees of negligence can be differentiated and may have a different weight for the overall assessment of an individual case. A low degree of negligence may have less of an impact on a decision to impose an administrative fine, while a high degree of negligence may indicate that the infringement is not minor and have a higher impact on the decision.

5.2.4 Article 83(2)(c) – Actions taken by controller or processor to mitigate damage suffered by data subjects

73 Controllers and processors have an obligation 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. In case of an infringement, the controller or processor should do whatever they can to reduce the consequences of the infringement for the individual(s) concerned. The adoption of appropriate measures to mitigate the damage suffered by the data subjects may be considered a mitigating factor in determining whether

the infringement may be minor and whether an administrative fine is the appropriate corrective measure.

74 When assessing the adopted measures, it is of particular importance to take into account the element of timeliness, i.e. the point in time when the measures are implemented by the controller or processor, and their effectiveness. 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.

5.2.5 Article 83(2)(d) – Degree of responsibility of the controller or processor

75 Pursuant to Article 83(2)(d) GDPR, the supervisory authority will assess the degree of responsibility of the controller or processor and will take into account measures implemented by them pursuant to Articles 24, 25 and 32 GDPR. In particular, the supervisory authority should assess to what extent the controller 'did what it could be expected to do'[49] given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the GDPR.

76 In particular, the supervisory authority should assess the residual risk for the rights and freedoms 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 24, 25 and 32 GDPR. The supervisory authority should take into account all the obligations of the GDPR, as well as the measures taken by the controller or processor. On this basis, the supervisory authority should then assess whether the before-mentioned residual risk, impairment and damage are sufficiently mitigated to ensure that all measures that could be required have been taken.

77 In this respect, the supervisory authority may also consider whether the data in question was directly identifiable and/or available without appropriate technical and organisational measures in accordance with Article 24, 25 and 32 GDPR. However, even if the data are not directly identifiable (such as pseudonymised data), this does not remove all responsibility from the controller or processor. It should be borne in mind that the existence of such measures does not necessarily constitute a mitigating factor. Given the fact that the GDPR imposes a high degree of responsibility on controllers and processors, the supervisory authority can consider this as a mitigating factor only in exceptional circumstances, where the controller or processor has gone above and beyond their obligations. This depends on all the circumstances of the case.

78 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 to be heard. 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 Data Protection Officer or data subjects (if applicable).

5.2.6 Article 83(2)(e) – Previous infringements by the controller or processor

79 Previous infringements are infringements already established before the decision is issued. In case of cooperation under Chapter VII GDPR, prior infringements are those already

[49] Calculation Guidelines, paragraph 77.

established before the draft decision (within the meaning of Article 60 GDPR) is issued. The supervisory authority is only required to take into account previous infringements that have been established before the communication of the preliminary findings to the controller or processor[50].

80 Pursuant to Article 83(2)(e) GDPR, 'any relevant previous infringements committed by the controller or processor' must be considered as an aggravating factor when assessing if the infringement is minor and deciding which measure to adopt. Supervisory authorities should consider that the scope of the assessment here can be quite wide because any type of infringement of the GDPR, though different in nature to the one currently being investigated by the supervisory authority might be 'relevant' (within the meaning of Article 83(2)(e) GDPR) for the assessment, as it could be indicative of a general level of insufficient knowledge or disregard for the data protection rules.

5.2.6.1 Time frame

81 In the first place, the supervisory authority should give regard 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 the supervisory authorities should consider it 'relevant' within the meaning of Article 83(2)(e) GDPR. Conversely, the more recently an infringement was committed, the more relevant for the supervisory authority in its assessment whether the infringement is minor and its decision to impose an administrative fine.

82 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 should not be set for this purpose. However, some national laws do prevent the supervisory authority from considering previous infringements after a certain period of time. In the same way, certain national laws impose a record deletion obligation after a certain period of time, which prevents the acting supervisory authority from taking into account these precedents.

5.2.6.2 Subject matter

83 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'.

84 Even though any prior infringements may provide an indication about the controller's or processor's general attitude towards the observance of the GDPR, infringements of the same subject matter should be considered more significant, as they are closer to the infringement currently under investigation. This is particularly the case when the controller or processor previously committed the same infringement (repeated infringements). Therefore, same subject-matter infringements should be considered more relevant than previous infringements concerning a different topic.

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

[50] Article 19(7) Regulation (EU) 2025/2518 of the European Parliament and of the Council of 26 November 2025 laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679.

5.2.6.3 Other considerations

86 As stated before, in the event of recurring infringements, the supervisory authority should consider all corrective measures as the repetition could be indicative of a general failure to ensure compliance with the GDPR. 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.

87 Previous infringements could also be considered when they were found by a different supervisory authority concerning the same controller or 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 or processor. Similarly, infringements previously determined by the lead supervisory authority could be taken into account when a different authority is handling 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 or processor.

88 The existence of previous infringements can be an aggravating factor when considering whether the infringement is minor and which measure to impose. The weight given to this factor is to be determined in view of the nature and frequency of the previous infringements. The mere absence of previous infringements by the controller or processor cannot, in itself, be considered a mitigating factor, as compliance with the GDPR is the norm.

Example 5: Recurring infringement no longer considered minor

An organisation processes data based on consent, notifying data subjects of new job opportunities that match their interests. The supervisory authority receives two complaints concerning cases where data subjects still received emails of the recruitment agency after they exercised their right to erasure of their personal data. Following a preliminary investigation by the supervisory authority, it was established that the controller maintained an internal policy regarding erasure requests and had instructed its recruiters accordingly. Consequently, the cases were considered to constitute a limited error. After issuing a reprimand to the organisation for not complying with the erasure requests, the supervisory authority received three more similar complaints. It turned out that the processor did have a procedure for handling requests to remove data. Yet in practice, it led to human errors in too many cases. Considering the recurring nature of the infringement the supervisory authority deemed that the infringement could no longer be considered minor and fined the controller.

5.2.7 Article 83(2)(f) – Degree of cooperation with the supervisory authority in order to remedy the infringement

89 Article 83(2)(f) GDPR 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.

90 Before further assessing the level of cooperation the controller or processor has established with the supervisory authority, it should be reiterated that a general obligation to cooperate is incumbent on the controller and the processor pursuant to Article 31 GDPR. It should therefore be considered that the ordinary duty of cooperation is mandatory. The GDPR does not provide discretion to consider mere cooperation as a mitigating factor, as this is already required.

91 However, in exceptional cases, where intervention of the controller has been mitigating in such a way that negative consequences on the rights of the data subjects did not occur or had a more limited impact than they otherwise could have had, this could also be taken into account as a mitigating factor. This also applies to the situation where exceptional cooperation with the supervisory authority has had the effect of limiting or avoiding negative consequences for the rights of the data subjects that otherwise might have occurred. 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 which has significantly limited the impact on the rights of the data subjects as a result. To be considered as a mitigating factor, the cooperation must go beyond what follows from applicable law or exceed what would normally be considered necessary.

5.2.8 Article 83(2)(g) – Categories of personal data affected

92 Concerning the categories of personal data affected (Article 83(2)(g) GDPR), the GDPR highlights the types of data that merit special protection and therefore a stricter way of enforcing. 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 where the dissemination of that data would cause immediate damage or distress to the data subject (e.g. location data, data on private communication, national identification numbers or financial data, such as transaction

overviews or credit card numbers)[51]. In general, the more of such categories of data involved or the more sensitive the data, the more likely it is that the infringement is not considered minor and, therefore, that an administrative fine should be imposed.

93 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.

5.2.9 Article 83(2)(h) – The manner in which the infringement became known to the supervisory authority

94 A supervisory authority might become aware of the infringement as a result of its own investigations, complaints, articles in the press, anonymous tips or notification by the controller.

95 Following Article 83(2)(h) GDPR, the manner in which the infringement became known to the supervisory authority could be a relevant factor to determine whether the infringement may be minor and which corrective measure is appropriate, if any. 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 otherwise became known to the supervisory authority. This circumstance is not relevant when the controller is subject to specific notification obligations (such as in the case of personal data breaches pursuant to Article 33 GDPR). In such cases, this notification should be considered as neutral.

96 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. However, the supervisory authority may consider this a mitigating factor if the controller or processor notified the infringement out of its own motion, prior to the supervisory authority's knowledge of the case.

5.2.10 Article 83(2)(i) – Compliance with measures previously ordered with regard to the same subject matter

97 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' should be considered when deciding whether to impose an administrative fine and deciding on its amount.

98 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.

99 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 controller or processor, it does not have any weight when assessing whether the infringement is minor and deciding whether to impose an administrative fine. Therefore, it does not preclude an administrative fine. On the contrary, a reinforced commitment on the part of the controller or processor in the fulfilment of previous

[51] Dissemination of private communications and location data can cause immediate damages or distress to the data subject, which has been highlighted by the special protection granted 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 judgment of the CJEU of 6 October 2020 in joined cases La Quadrature du Net et al, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 117 and the case law there cited.

measures is required for this factor to apply as mitigating, e.g. taking additional measures beyond those ordered by the supervisory authority.

100 Conversely, non-compliance with a corrective measure previously ordered is aggravating and generally illustrates that the infringement is not minor and that it is more appropriate to impose an administrative fine. Alternatively, this could be seen as a different infringement in itself, pursuant to Article 83(5)(e) and Article 83(6) GDPR. In any case, due note should be taken that the same non-compliant behaviour cannot lead to a situation where it is punished twice.

5.2.11 Article 83(2)(j) – Adherence to approved codes of conduct or approved certification mechanisms

101 Adherence to approved codes of conduct may be used by the controller or processor as a way to demonstrate compliance.

102 In case of an infringement of one of the provisions of the GDPR, adherence to an approved code of conduct might be indicative of whether the infringement is minor and to what extent the supervisory authority needs to impose an administrative fine and/or other corrective measure. Approved codes of conduct will, pursuant to Article 40(4) GDPR, contain 'mechanisms which enable the (monitoring) body to carry out mandatory monitoring of compliance with its provisions'.

103 In cases where a controller or processor adhered to a code of conduct and the monitoring body in charge of administering the code takes appropriate action against their member, the supervisory authority may refrain from imposing additional measures in order to ensure that the measures are sufficiently effective, proportionate and dissuasive. Nevertheless, the powers of the monitoring body are 'without prejudice to the tasks and powers of the competent supervisory authority' (Article 41(4) GDPR), which means that the supervisory authority is not under an obligation to take into account previously imposed sanctions pertaining to the self-regulatory scheme.

104 However, if failure to comply with the codes of conduct or certification is directly relevant to the infringement, the supervisory authority may consider that the infringement is not minor and that an administrative fine is more likely to be issued.

5.2.12 Article 83(2)(k) – Other aggravating and mitigating circumstances

105 The provision itself gives examples of which other elements might be taken into account when deciding the appropriateness of an administrative fine for an infringement of the provisions mentioned in Article 83(4) to (6) GDPR.

106 Information about profit obtained or losses avoided as a result of an infringement may be particularly important for the supervisory authority as economic gain from the infringement cannot be compensated through measures that do not have a pecuniary component. As such, the fact that the controller has profited from the infringement of the GDPR may constitute a strong indication that the infringement is not minor and that an administrative fine should be imposed.

107 The scope of this provision, which is necessarily open-ended, should include all the reasoned considerations regarding the social and economic context in which the controller or processor operates, those relating to the legal context and those concerning the market context[52]. In particular, economic gain from the infringement could be a strong indicator that the

[52] See paragraphs 108 and 109 of the Calculation Guidelines, as well as EDPB Binding Decision 2/2022 paragraph 207 and EDPB Binding Decision 3/2022, paragraph 368.

infringement is not minor and that an administrative fine is more likely to be issued, if the case provides information about profit obtained as a result of the infringement of the GDPR. Exceptional circumstances that could lead to significant changes in the socio-economic context (e.g. the onset of a serious emergency that could radically change the way processing of personal data is carried out) could also be considered under Article 83(2)(k) GDPR.

5.2.13 Practical examples of minor infringements

Example 6: Failure to respond to a data subject access request

The supervisory authority found that an SME had infringed Article 12(3) GDPR by not informing a complainant without undue delay of the outcome of their request for access and Article 15 GDPR by failing to inform them that it did not process their personal data. The supervisory authority found that the infringements were minor within the meaning of Recital 148 GDPR and that it was appropriate to issue a reprimand pursuant to Article 58(2)(b) GDPR based on the following relevant facts.

The investigation covered the SME's handling of one individual complainant's request for access. The SME had stated that they had not received the request but that it was possible that it had ended up in their spam folder. Furthermore, the SME could now upon further review not find any data on the complainant. The following were considered to be mitigating factors: The SME had provided the complainant with a written apology and informed them that it had not processed any information relating to them and clarified how the complainant could get in touch with the correct controller. The SME had not previously been in contact with the data subject in question, which makes it more understandable that it went to the spam folder. Neither had anything similar happened before, which made the SME less prone to check their spam folder. The SME immediately dealt with the request after the supervisory authority contacted it. Furthermore, the identified infringements have occurred relatively far back in time. A somewhat aggravating factor was that the complainant's right of access had been left unanswered until the initiation of the supervisory authority's investigation, which might have been due to a temporary failure in the SME's mail system.

Example 7: Failure to implement systematic procedures for third-party tracking tools

The supervisory authority found that an SME had infringed Article 32(1) GDPR by not implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk when using a tracking pixel from a social media provider in a service offer on a webpage for a service used for video conferencing meetings between businesses and their customers. The supervisory authority found that the infringement was minor within the meaning of Recital 148 GDPR and that it was appropriate to issue a reprimand pursuant to Article 58(2)(b) GDPR based on the following relevant facts.

The infringement concerned the unintentional transfer of hashed contact details (email addresses and phone numbers) of approximately 50,000 users to the social media provider over a two-year period. The transfer occurred because a certain technical function was activated in the social media provider's developer tool, which took precedence over the data protection settings the organisation had configured in its own Customer Data Platform. The supervisory authority noted that the SME lacked the systematic procedures required to identify such unintentional changes, as the incident was only discovered following a report from a third party. Although quite a large data set, the transferred data was hashed, and thus unusable, and for instance did not include any sensitive data, such as special categories of personal data or information regarding the context of the meetings. Furthermore, the SME had implemented other data protection measures that limited the scope of the data collection and the incident did not involve an uncontrolled public disclosure, even though the SME failed to activate the relevant function.

Example 8: Failure to respond to a data subject access request

The supervisory authority found that a controller had infringed Article 15 GDPR by establishing that the conditions for refusing access under Article 15(4) GDPR were not met, as the controller had not demonstrated that the alleged impact on the rights of others could not be mitigated by appropriate measures. The supervisory authority found that the infringement was minor within the meaning of Recital 148 and that it was appropriate to issue a reprimand pursuant to Article 58(2)(b) GDPR based on the following relevant facts.

The processing concerned the operation of video surveillance of a parking facility managed by a company owned by the municipality. The individual exercised the right of access under Article 15 GDPR by requesting access to a video recording showing a vehicle specified in the request. The controller refused access, arguing that granting a copy would adversely affect the rights and freedoms of other individuals, since identifying the relevant footage would require reviewing numerous recordings containing vehicles with visible registration numbers, thereby interfering with the privacy of third parties. Yet, the complainant had stated that access in a timely manner was essential for a civil claim regarding an accident, which was subsequently statute barred.

The investigation following the complaint focused on the controller's failure to ensure compliance with the complainant's right to access in the circumstances of this case. When assessing liability, the supervisory authority took into account several mitigating circumstances. The supervisory authority considered that the infringement was limited in scope and duration. The controller acted with a low degree of negligence and took action immediately after being contacted by the supervisory authority. They reached out to the individual and was in that way able to narrow down the

time frame of the footage needed to address the access request. They also implemented software enabling them to blur registration numbers and, by doing so, further mitigate the impact on the rights of others (including as regards similar access requests for the future).

Example 9: Transparency deficiencies subject to special mitigating circumstances

The supervisory authority found that a non-profit organisation (a small sports club) had infringed the transparency and information obligations laid down in Articles 12 and 13 GDPR in processing operations carried out in the context of offering a fan page, by having transmitted certain data to a third party, that could not be regarded as anonymous within the meaning of the GPPR, but qualified as pseudonymised data. The supervisory authority found that the infringement was minor within the meaning of Recital 148, and that it was appropriate to issue a reprimand pursuant to Article 58(2)(b) GDPR based on the following relevant facts.

The information provided to users did not accurately reflect the applicable legal qualification of the data, nor did it fully specify the relevant processing purposes and legal bases. The supervisory authority considered in an overall assessment that the infringement resulted from a faulty legal assessment rather than intentional non-compliance. The supervisory authority also considered the prompt and effective safeguards and compliance measures adopted, including the revision of the privacy policy to reflect the pseudonymised nature of the data, the clarification of applicable purposes and legal bases, and the implementation of technical measures aimed at minimising the risk of re-identification.

Example 10: No longer a minor infringement

The supervisory authority found that a small telecommunications company, had responded to a data subject's request for information with a month's delay, contrary to the requirements in Article 12(3) and (4) GDPR, without giving advance notice of the long processing time. At first, the supervisory authority found that the infringement was minor within the meaning of Recital 148 GDPR and that it was appropriate to issue a reprimand pursuant to Article 58(2)(b) GDPR, given that the delay was relatively brief and the information was subsequently provided in full.

While handling the initial individual complaint, the supervisory authority became aware of further identical cases and initiated administrative fine proceedings against the company based on the following relevant facts.

Although a one-time delay might be considered as minor, the accumulation of many cases suggests that the delayed response is not an exception, but rather a fundamental problem or pattern that can no longer be considered as

a minor infringement. The accumulation of cases therefore leads to the assessment that an administrative fine is appropriate.

5.3 Step 5: Would the imposition of an administrative fine be effective, proportionate and dissuasive?

5.3.1 Effectiveness, proportionality and dissuasiveness

108 The next step for the supervisory authority is to assess whether the imposition of an administrative fine would be effective, proportionate and dissuasive in the individual case in accordance with Article 83(1) GDPR. Depending on whether the established infringement is considered as minor in step 4 (Section 5.2), the supervisory authority will move on to either step 5 a (Section 5.3.2) or step 5 b (Section 5.3.3) in order to determine whether to impose an administrative fine. In both these steps, the supervisory authority should have due regard to these three overarching criteria for the imposition of administrative fines.

109 These criteria are relevant for the calculation of an administrative fine. This means that the amount of a fine must be tailored to the infringement committed in its specific context[53]. These criteria are also relevant for deciding whether to impose an administrative fine to begin with, which is clear from the content of that provision and the objective pursued. As for the context, due regard shall be given to the mitigating and aggravating factors in Article 83(2) GDPR, both when deciding whether to impose an administrative fine and when calculating it. These factors serve to ensure that each infringement is assessed on the basis of all the relevant individual circumstances and that the objectives pursued by the system of penalties provided for in the GDPR are achieved[54]. As for the objectives pursued, administrative fines have a punitive function and purpose[55].

110 In general, this means that supervisory authorities must ensure that they use administrative fines, like all other corrective measures, in a way that adequately responds to the specific infringement, assess all the facts in a manner that is consistent and objectively justified, and maintain the objective pursued. The three overarching criteria support this. The assessment of what is effective, proportionate and dissuasive in each case will have to also reflect whether the objective pursued by the corrective measure chosen is to establish compliance with the rules, punish unlawful behaviour or both.

111 Rules laying down penalties are *effective* where they are framed in such a way that they do not make it practically impossible or excessively difficult to impose the penalty provided for, and, therefore, to attain the objectives pursued by EU law. In this context, the principle of effectiveness means that although national legislation may set additional requirements on the enforcement procedure to be followed by the supervisory authorities (such as address notifications or deadlines for making representations, filing appeals or payment of a fine), such requirements should not hinder the achievement of effectiveness, proportionality or dissuasiveness in practice.

112 A penalty is *dissuasive* where it prevents an actor from infringing the objectives pursued and rules laid down by EU law. What is decisive in this regard is not only the nature and level of the penalty but also the likelihood that it will be imposed. Anyone who commits an infringement must fear that the penalty will in fact be imposed on them. This criterion is of particular

[53] See Calculation Guidelines, paragraph 132.
[54] C-383/23, ILVA, paragraph 28.
[55] C-667/21, Krankenversicherung Nordrhein, paragraph 85; judgment of the CJEU of 4 September 2025, Quirin Privatbank, C-655/23, EU:C:2025:655, paragraph 70 and the case-law cited.

relevance to administrative fines due to their punitive function and purpose, which make them in particular aimed at both 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). The principle of *dissuasiveness* means that the supervisory authority should establish and maintain a practice of imposing administrative fines to a degree which provides a substantial disincentive to anyone considering to commit an infringement intentionally or to abstain from taking appropriate compliance measures to prevent negligent infringements. Particularly as regards general deterrence, such a practice aims to encourage compliant behaviour to avoid the imposition of an administrative fine.

113 Finally, a penalty is *proportionate* where it is appropriate (i.e. effective and dissuasive) for attaining the legitimate objectives pursued by it, and also necessary. Where there is a choice between several (equally) appropriate penalties, to the supervisory authority should impose the one which is the least onerous. Moreover, the effects of the penalty on the person concerned must be proportionate to the aims pursued[56]. In this context, the principle of proportionality means that the decision to impose an administrative fine in a particular case 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). Lastly, the seriousness of the infringement is an important element to take into account when assessing the proportionality of a corrective measure, such as whether to impose an administrative fine[57].

5.3.2 Step 5 a: The infringement is considered minor – an administrative fine should not be imposed

114 If the supervisory authority finds that the seriousness of the established infringement is minor in step 4 (Section 4.1), it will move on to step 5 a.

115 As explained above[58], the consequence of an infringement being considered minor is that, as a general rule, an administrative fine will not be imposed, whereas a reprimand may be issued instead. However, even when the seriousness of the established infringement is considered as minor, the EDPB does not exclude that a supervisory authority could still use its discretion to impose an administrative fine[59]), taking into consideration the circumstances of the individual case, as well as the principles of effectiveness, dissuasiveness and proportionality[60].

116 Furthermore, in some cases of a minor infringement, it may not be appropriate, necessary or proportionate to exercise any corrective power under Article 58(2) GDPR.

117 The CJEU has ruled that, when an infringement of the GDPR has been established, the supervisory authority is required to take action where the exercise of one or more of the corrective powers provided for in Article 58(2) GDPR is, taking into account the circumstances of the specific case, appropriate, necessary and proportionate to remedy the shortcoming found and ensure that the GDPR is fully enforced[61]. However, the GDPR leaves the

[56] Judgment of the General Court of 26 October 2017, Marine Harvest v Commission, T-704/14, EU:T:2017:753, paragraph 580, referencing judgment of the General Court of 12 December 2012, Electrabel v Commission, T-332/09, EU:T:2012:672, paragraph 279.
[57] See EDPB Binding Decision 1/2023, paragraph 259, EDPB Binding Decision 1/2021, paragraph 256 and EDPB Binding Decision 4/2022, paragraph 280.
[58] See Section 5.1.
[59] In addition to, or instead of, other corrective measures under Article 58(2) GDPR.
[60] Where the supervisory authority decides to impose an administrative fine for an established infringement of the GDPR, it should refer to the Calculation Guidelines for the calculation of the fine.
[61] C-768/21, Land Hessen, paragraph 42. See also Recital 129 GDPR, where it is stated that each measure should in particular be appropriate, necessary and proportionate in view of ensuring compliance with the regulation, considering the circumstances of each individual case.

supervisory authority a discretion as to which corrective measure to adopt[62]. Furthermore, the supervisory authority is not under an obligation to exercise a corrective power in all cases where it finds an infringement[63]. For example, the supervisory authority could, in light of the circumstances of the specific case, refrain from taking a corrective measure where the controller has, as soon as it became aware of an infringement, taken appropriate and necessary measures to ensure that the infringement is brought to an end and does not recur[64].

Example 11: Unlawful access by employee to customer personal data

Following the notification of a data breach, the supervisory authority found that a savings bank had infringed Article 32 GDPR regarding the security and processing of a customer's personal data (unlawful access and short retention period for access logs), but that it had not infringed Article 34 GDPR regarding the obligation to notify the data subject of the data breach. However, the supervisory authority determined not to exercise any of its corrective powers, despite the established infringement, as it found that action on the part of the supervisory authority was not appropriate, necessary or proportionate in that specific case.

The infringement concerned an employee of the savings bank who had, on several occasions, unlawfully accessed the personal data of the complainant. The savings bank had notified the supervisory authority of the breach pursuant to Article 33 GDPR but had not informed the data subject, assessing that the breach was unlikely to result in a high risk to their rights and freedoms. The complainant also objected to the savings bank's short retention period for access logs.

Relevant facts supporting the supervisory authority's decision to refrain from further action included that the infringement had not continued and that the controller had taken immediate measures to remedy the situation. Specifically, disciplinary measures had been taken against the employee, who confirmed in writing that they had not copied or transferred the data to third parties and committed not to repeat the conduct. Furthermore, in response to the supervisory authority's investigation regarding the access logs, the savings bank had committed to reviewing and extending the retention period. Consequently, the supervisory authority considered that the controller had autonomously ensured the infringement was brought to an end and would not recur.

Example 12: Failure to update transparency statement for an incidental processing of personal data

The supervisory authority found that an SME had infringed Article 13 GDPR

[62] C-768/21, Land Hessen, paragraph 37.
[63] C-768/21, Land Hessen, paragraph 41, where it is also clarified that, in those circumstances, a complainant whose rights have been infringed does not have a subjective right to seek the imposition by the supervisory authority of an administrative fine on the controller.
[64] C-768/21, Land Hessen, paragraph 43.

by not updating their transparency statement. The supervisory authority found that the infringement was minor within the meaning of Recital 148 GDPR, but that it would not be proportionate to exercise a corrective power based on the following relevant facts.

An SME intended to implement a one-time raffle amongst its customers. Although the SME processed the data in a lawful manner, it failed to update its transparency statement. The supervisory authority was subsequently notified of the omission via a complaint submitted by a data subject. Before the supervisory authority initiated an investigation, the SME amended its transparency statement and brought it in line with the requirements of the GDPR. The non-compliance was remedied and the infringement was brought to an end.

Example 13: Personal data leaked due to a human error and insufficient organisational measures

The supervisory authority found that a controller had infringed Article 32 GDPR by not taking sufficient technical and organisational measures. Although the supervisory authority established a minor infringement within the meaning of Recital 148 GDPR, it found that it would not be proportionate to exercise a corrective power based on the following facts.

A controller accidentally disclosed a copy of a data subjects driver's license after an employee mistakenly included the file in an email sent to a limited number of other data subjects. The controller notified both the supervisory authority and the data subject without delay. The controller reimbursed the total costs that the data subject incurred to replace the compromised document. Without waiting for the supervisory authority's decision on whether an investigation would be required, the controller immediately hired a third party to re-evaluate its technical and organisational measures. This assessment revealed that it did not implement sufficient measures to ensure that human errors would not take place. As a result, the controller adopted more technical and organisational measures to ensure that another incident would not occur in the future.

5.3.3 Step 5 b: The infringement is not considered minor – an administrative fine should be imposed

118 If the supervisory authority finds that the seriousness of the established infringement is not minor in step 4 (Section 4.1), it will move on to step 5 b.

119 As explained above[65], the consequence of an infringement not being considered minor is that, as a general rule, an administrative fine, will be imposed. However, even when the seriousness of the established infringement is not considered as minor, the supervisory authority still has the discretion to take other corrective measures under Article 58(2) GDPR

[65] See Section 5.1.

(in addition to, or instead of, an administrative fine)[66], such as a reprimand. This decision needs to be made based on the circumstances of the individual case and taking the principles of effectiveness, dissuasiveness and proportionality into account.

120 As previously mentioned[67], depending on the circumstances in a specific case, the supervisory authority may, for example, choose to issue a reprimand instead of an administrative fine, where the fine likely to be imposed for an infringement not considered as minor would constitute a disproportionate burden to a natural or legal person. Furthermore, in Member States where national legislation does not allow for the imposition of administrative fines in relation to public authorities, a reprimand (or other measures established by national law) may be issued instead of an administrative fine, even when the infringement is not considered as minor.

Example 14: Processing of special category data under constitutional protection

The supervisory authority found that an organisation had infringed Article 9 GDPR by processing health data without a valid exemption under Article 9(2) GDPR. The supervisory authority found that the infringement was not minor within the meaning of Recital 148 GDPR, but that the imposition of an administrative fine would not be proportionate. Instead, it found that it was appropriate to issue a reprimand pursuant to Article 58(2)(b) GDPR based on the following relevant facts.

The infringement concerned the extensive collection and publication on a website of health data concerning a large number of data subjects by collecting and publishing rulings concerning them on compulsory care from administrative courts related to psychiatric illness or substance abuse. However, the collection and publication had been carried out within an operation that had been granted a certificate of publication from a public authority which normally would make it exempt from that obligation under national constitutional law. A limitation of constitutional protection for such processing had been introduced relatively recently and not previously applied by national authorities or courts. There was also widespread debate on and misunderstandings about how to apply the law. Therefore, there was a lack of practice on how the constitutional provision – which in some respects requires relatively difficult considerations – should be applied. In addition, the supervisory authority had guiding information on its website that could be perceived as meaning that the supervisory authority had no possibility of intervening against actors with such certificates of publication.

121 As explained above, and as held by the CJEU[68], the supervisory authority is not required to exercise any corrective power under Article 58(2) GDPR, where such action is not appropriate, necessary or proportionate to remedy the shortcoming found and to ensure that the regulation is fully enforced[69]. Taking this into account, the EDPB does not exclude that a supervisory

[66] See Section 3.
[67] See paragraph 26.
[68] See Section 5.3.2, including C-768/21, Land Hessen.
[69] As mentioned in Section 3.2, it should be recalled in this context that the supervisory authority has the responsibility of choosing the most appropriate corrective measure(s). In the cases mentioned in Article 83(4)–(6) GDPR, this choice should include consideration of all of the corrective measures, including the imposition of an administrative fine, either accompanying a corrective measure under Article 58(2) GDPR or on its own.

authority could, in exceptional circumstances, refrain from exercising a corrective measure also in a situation where the established infringement is not considered minor. However, the EDPB assumes that, in such a situation, where concluding that an administrative fine would not be appropriate, necessary or proportionate, the supervisory authority would, in general, use its discretion to issue a reprimand instead of a fine, rather than to refrain from exercising any corrective measure.

122 Where a supervisory authority decides to impose an administrative fine for an established infringement of the GDPR, it should refer to the Calculation Guidelines for the calculation of the fine.

Annex 1 Methodology for determining whether to impose an administrative fine