VILNIAUS STR. 31
01402 VILNIUS
LITHUANIA

T. +370 5 231 2211
E. INFO@TRINITI.LT
WWW.TRINITI.LT

E. DELIVERY BOX
ADDRESS
306233023

TRINITI
TALLINN RIGA VILNIUS

To the European Data Protection Board

REGARDING COMMENTS ON GUIDELINES 04/2026 ON THE APPLICATION OF THE POWER TO IMPOSE ADMINISTRATIVE FINES IN RELATION TO OTHER CORRECTIVE POWERS UNDER THE GDPR

Vilnius, 2026-11-13

Following the publication for public consultation by the European Data Protection Board (hereinafter referred to as the EDPB) of the Guidelines 04/2026 on the application of the power to impose administrative fines in relation to other corrective powers under the GDPR (hereinafter referred to as the Guidelines), we would like to express our support for the EDPB's efforts to harmonise the methodology for deciding whether an administrative fine should be imposed in addition to, or instead of, other corrective measures. We welcome, in particular, the clear five-step structure, the clarification of the criteria for assessing whether an infringement qualifies as minor, and the inclusion of practical examples illustrating the application of different corrective measures.

At the same time, based on our practical experience advising organisations of different sizes on compliance with 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 referred to as the GDPR), we would like to submit the following observations and recommendations for consideration. Attention is given to the position of small and medium-sized enterprises (SMEs), for which an administrative fine may have a disproportionate or even existential effect, while the main objective, a durable state of compliance, could often be achieved by other means.

1. THE STRONG PRESUMPTION IN FAVOUR OF A FINE SHOULD BE BALANCED BY PROPORTIONALITY

The Guidelines provide that, where an infringement is not considered minor, there is a strong presumption to impose an administrative fine. In our view, this formulation risks leading to an almost automatic imposition of fines without sufficient individual assessment and may in practice limit the discretion that Article 83(2) GDPR and Recital 148 GDPR leave to supervisory authorities. We would recommend clarifying that the presumption is a starting point for the assessment under Article 83(1) GDPR, rather than a rule, and that the choice of the least onerous of several equally appropriate measures remains a mandatory part of Step 5, as reflected in paragraph 113 of the Guidelines.

2. THE SIZE AND ECONOMIC CAPACITY OF THE ADDRESSEE SHOULD BE AN EXPLICIT CRITERION

The Guidelines recognise, in paragraphs 26 and 120, that a reprimand may be issued where a fine would constitute a disproportionate burden to a legal person. However, the size and economic capacity of the controller or processor are not identified as factors for systematic assessment under Step 5. We recommend expressly including these considerations in Step 5, so that supervisory authorities assess, in a consistent manner, whether a fine would impose a disproportionate financial burden on an SME, potentially threatening its economic viability, and whether the objectives of the GDPR could be achieved equally effectively by other corrective measures.

3. THE ASSESSMENT OF NEGLIGENCE SHOULD TAKE INTO ACCOUNT THE POSITION OF SMES

The Guidelines state that where EDPB Guidelines exist, an error is always to be considered avoidable and therefore at least negligent. Given the volume and technical complexity of EDPB and national guidance, it may not be realistic to expect every SME to identify and correctly interpret all relevant guidance. We would suggest that this rule apply only to final, rather than draft, guidelines, and that the Guidelines clarify that the degree of negligence, which the Guidelines themselves recognise as relevant under Step 4, should take into account the resources and expertise reasonably available to the addressee.

For example, a small online retailer with five employees and no in-house legal or data protection expertise uses a standard e-commerce platform and configures its newsletter sign-up form in line with the platform's default settings. A supervisory authority later finds that the information provided under Article 13 GDPR was incomplete, on the basis of an interpretation set out in EDPB guidelines. Under the current wording, the error would automatically be considered avoidable and therefore at least negligent, in the same way as for a large undertaking with a dedicated compliance function which actively follows EDPB publications. In our view, in such a case the draft status of the guidance, the limited resources of the retailer and its reliance on the platform's standard configuration should at least be reflected in a lower degree of negligence when assessing whether the infringement is minor and which corrective measure is appropriate.

4. RELIANCE ON DOCUMENTED PROFESSIONAL ADVICE SHOULD BE CLARIFIED

The Guidelines explain that external or internal legal advice cannot, as such, exculpate the controller, in particular where it is not documented or is followed blindly. SMEs typically rely on external advisers rather than in-house expertise. We would recommend clarifying what level of documentation is expected and that good faith reliance on documented advice, obtained on the basis of complete facts and reasonably relied upon in light of the available legal guidance, may be taken into account as a factor reducing the degree of negligence, even if it does not exclude culpability.

5. MITIGATING FACTORS SHOULD NOT BE LIMITED TO EXCEPTIONAL SITUATIONS

Under the Guidelines, technical and organisational measures may be considered mitigating only in exceptional circumstances, where the controller has gone above and beyond its obligations, ordinary cooperation is not considered mitigating, and a notification under Article 33 GDPR is considered neutral. Combined with the broad scope given to aggravating factors, this creates an asymmetry which particularly affects SMEs, which rarely have the resources to exceed their legal obligations. We recommend that timely, effective and documented remediation, especially when undertaken spontaneously before an investigation, be given meaningful weight as a mitigating factor under Article 83(2)(c) GDPR, where it effectively reduces the consequences of the infringement.

6. COMPLIANCE ORDERS WITH VERIFICATION SHOULD BE RECOGNISED AS AN ALTERNATIVE TO A FINE

The Guidelines recognise that orders under Article 58(2)(d) GDPR may require processing to be brought into compliance in a specified manner and within a specified period, and that non-compliance with such orders is an aggravating factor or a separate infringement. In our view, the Guidelines could expressly recognise that, particularly for SMEs, an order requiring specific and proportionate measures (for example, where appropriate, an independent audit, implementation of its recommendations and submission of evidence of implementation), combined with subsequent verification, may be an effective and proportionate alternative to a fine where the infringement is not minor but a fine would be disproportionate. Such an approach would direct the SME's resources towards compliance, while the possibility of further sanctions in the event of non-compliance would contribute to the dissuasive effect.

7. GUIDANCE ON THE TIME RELEVANCE OF PREVIOUS INFRINGEMENTS SHOULD BE MORE CONCRETE

Paragraphs 81 and 82 of the Guidelines state that the significance of a previous infringement decreases over time, while rejecting fixed limitation periods. We acknowledge this approach; however, without any indicative benchmark, it remains difficult for addressees, particularly SMEs, to anticipate how long a previous infringement may continue to weigh against them. As illustrated by the examples, a reprimand for a minor infringement may effectively become the basis for a fine in subsequent proceedings. We would recommend providing indicative guidance on the time frame within which previous infringements are generally considered relevant, and clarifying that minor infringements resulting in a reprimand should carry limited weight after a reasonable period, in order to ensure legal certainty.

8. THE LIABILITY OF SMES FOR PROCESSORS SHOULD BE ASSESSED IN CONTEXT

The Guidelines confirm that a controller is liable for infringements committed by a processor acting on its behalf. SMEs frequently rely on large technology providers offering standardised terms which they cannot negotiate or effectively audit. We would recommend clarifying that, when assessing the degree of responsibility under Article 83(2)(d) GDPR, supervisory authorities should take into account the controller's realistic ability to influence the processor's measures and the diligence exercised in selecting the processor.

9. ADHERENCE TO APPROVED CODES OF CONDUCT AND CERTIFICATION MECHANISMS SHOULD BE RECOGNISED AS MITIGATING FOR SMES

The Guidelines take adherence to an approved code of conduct into account mainly where the monitoring body has already acted, while non-compliance with a relevant code may indicate that a fine is more likely. For SMEs, approved codes of conduct and certification mechanisms are among the most practical and cost-effective means of demonstrating compliance. We would recommend that genuine adherence to a relevant approved code or certification be expressly recognised as a mitigating factor for SMEs, and that the development of SME-specific codes be actively encouraged, in line with Article 40(1) GDPR.

10. MORE SME-SPECIFIC EXAMPLES WOULD BE USEFUL

We welcome the examples in which SMEs received a reprimand or no corrective measure was imposed. We would encourage the EDPB to add examples where an infringement by an SME is not considered minor, yet a reprimand combined with a compliance order may be considered more appropriate than a fine, as well as examples showing how remediation measures taken by an SME are reflected in Steps 4 and 5.

11. THE DIFFERING TREATMENT OF PUBLIC AND PRIVATE SECTOR ADDRESSEES SHOULD BE ADDRESSED

The Guidelines acknowledge that, pursuant to Article 83(7) GDPR, Member States may determine whether and to what extent administrative fines may be imposed on public authorities and bodies, and that a reprimand may be issued instead of a fine where national law does not allow fines, even when the infringement is not considered minor. In practice, public bodies, which frequently process large volumes of personal data, including special categories of data and data of vulnerable persons, may be exempt from fines or subject to lower statutory limits under national law. In our experience, this has a discriminatory effect and also weakens the incentive for public bodies to implement appropriate technical and organisational measures. Public bodies may justify insufficient security or compliance measures by a lack of budget allocation. An SME, however, cannot rely on the same argument: under the Guidelines, the controller must do what it could be expected to do in light of its obligations, measures are considered mitigating only where the controller has gone above and beyond them, and Article 32 GDPR does not allow

the cost of implementation to justify a level of security below what the risk requires. As a result, the same lack of resources is treated as an excuse for a public body, but not for a private company which equally cannot afford costly technology or specialists.

While we recognise that Article 83(7) GDPR falls outside the scope of the Guidelines, we would recommend that the Guidelines (i) confirm that Steps 1 to 5, including the assessment of whether an infringement is minor, apply to public and private sector addressees in the same manner; (ii) state expressly that insufficient budget or funding cannot be considered a mitigating factor or a reason to refrain from corrective measures, for public bodies and private entities alike; (iii) clarify that, where a fine cannot be imposed or is limited by national law, the supervisory authority should not limit itself to a reprimand for infringements which are not minor, but should rather use binding orders with deadlines and subsequent verification, limitations or bans, so that the absence of a fine does not result in the absence of compliance; and (iv) include at least one example of an infringement by a public body which is not minor and the corrective measures considered appropriate in such a case. We would also invite the EDPB, in a future revision of the Calculation Guidelines, to consider whether guidance on an appropriate reference value for public bodies (for example, the annual budget allocation) could be provided, so that, where national law allows fines, they remain effective, proportionate and dissuasive.

OVERALL RECOMMENDATION

The Guidelines provide a valuable and structured methodology which will contribute to consistent enforcement across the EU. However, without clearer proportionality guidance, there is a risk that the strong presumption in favour of a fine, the low negligence threshold and the restrictive approach to recognising mitigating factors may lead to outcomes that are disproportionate for SMEs and do not necessarily improve compliance. We would therefore encourage the EDPB to retain the dissuasive function of administrative fines while expressly recognising the size and economic capacity of the addressee, effective remediation and verified compliance orders as legitimate elements of the assessment, and ensuring that comparable infringements by public and private sector addressees lead to comparably effective corrective measures, without lack of resources being accepted as an excuse for one group but not the other.

Best regards,

APB TRINITI

Lithuania