# Response to the EDPB public consultation on Guidelines 04/2026

## About Bending Spoons

Bending Spoons S.p.A. was founded in 2013 by five young friends with technical backgrounds and entrepreneurial ambitions. Today, it has grown into a group of companies (together, "**Bending Spoons**") that acquire and improve digital businesses, including Airtable, AOL, Brightcove, Eventbrite, Evernote, Miro, WeTransfer, and Vimeo.

Our businesses have served over a billion people worldwide, with around 500 million monthly active users and 9 million monthly paying customers. As our users are located around the world, we operate under multiple privacy and data protection frameworks and engage with government and regulatory authorities across the European Economic Area ("**EEA**") and other jurisdictions.

When we acquire a business, we typically restructure it and strengthen its privacy and security practices, among other interventions. We see data protection as part of product quality, and we invest in it accordingly.

## Our view on the Draft Guidelines

### High-level view

Bending Spoons welcomes the draft *Guidelines 04/2026 on the application of the power to impose administrative fines in relation to other corrective powers under the GDPR* ("**Draft Guidelines**").

Companies operating across the EEA face a fragmented legal landscape. The laws regarding privacy and data protection overlap at both European and national level, and global companies must also reconcile them with the laws of other jurisdictions. Moreover, supervisory authorities have taken different positions on the same issues. As a result, companies must spend significant time and resources reconciling these overlapping requirements and diverging positions, at the expense of focusing on innovation and product development.

In this context, clear and predictable criteria on when a fine is appropriate are essential to ensure a consistent enforcement framework across the EEA. They also allow companies to understand what is expected of them and to direct their resources where they matter most for data subjects.

# Our recommendations

The methodology outlined in the Draft Guidelines uses the factors in Article 83(2) of the Regulation (EU) 2016/679 ("**GDPR**") to determine whether an infringement is minor (step 4), and to assess whether an administrative fine would be effective, proportionate, and dissuasive, or whether another corrective measure would be more appropriate (step 5). Our recommendations aim to ensure that, at both stages, these factors can operate as mitigating as well as aggravating factors.

We first address how supervisory authorities should assess the infringement, with a focus on the diligence exercised by the controller. We then turn to the legal context in which controllers operate and the remediation they may undertake, which should be considered in deciding on the appropriate measure.

## Assessing the infringement

### The diligence of the controller

Accountability is one of the cornerstones of the GDPR. Controllers are expected to put in place governance structures, risk assessments, audits, security measures, and staff training, and to be able to demonstrate them. We agree that compliance with these obligations is the norm, and paragraph 75 rightly asks supervisory authorities to assess whether the controller did what it could be expected to do. The diligence a controller actually exercises should be reflected both in the degree of its negligence under Article 83(2)(b) of the GDPR and in the degree of its responsibility under Article 83(2)(d) of the GDPR, as set out below:

- **Governance and compliance measures**. Paragraph 77 states that the measures adopted by a controller can be considered mitigating only in exceptional circumstances, where the controller has gone "above and beyond" its obligations. The Draft Guidelines do not explain what this means in practice. In a risk-based framework, where the required measures already depend on the context of each processing, it is difficult to identify when measures would qualify as going beyond those obligations, creating uncertainty as to when the standard can apply. If inadequate measures increase the degree of responsibility, robust measures should be able to reduce it. Otherwise, a controller that has invested significantly in compliance would be assessed in the same way as one that has done the minimum.

  We propose replacing the last three sentences of paragraph 77 with the following:

  "The mere existence of measures required by the GDPR does not in itself constitute a mitigating factor. However, where the controller or processor has implemented robust and documented measures appropriate to the risk and relevant to the infringement, and did

what it could be expected to do in light of the nature, scope, context, and purposes of the processing, this indicates a low degree of responsibility under Article 83(2)(d) of the GDPR and may be taken into account as a mitigating factor."

## Identifying the corrective measure

### A fragmented legal context

The GDPR aims to ensure consistent protection across the EEA. In practice, however, controllers often operate in a fragmented legal context. Supervisory authorities sometimes take different positions on the same issue, including in cross-border cases, and companies operating globally are subject to third-country laws whose obligations, such as on data retention or age verification, cannot always be reconciled with the GDPR. This does not lower the level of protection the GDPR requires, but should affect how a controller's conduct is assessed and which corrective measure is most appropriate.

Paragraph 107 of the Draft Guidelines already recognises that Article 83(2)(k) of the GDPR covers considerations relating to the legal context in which the controller operates. The final Guidelines should make explicit that this context includes both diverging positions among supervisory authorities and genuine or potential conflicts with third-country law, and that, where the controller has acted diligently in such circumstances, these elements can operate as mitigating factors.

In Example 4(b), negligence follows from disregarding the known position of a supervisory authority. The same logic should work in the controller's favour where it follows a position. Likewise, without calling Article 48 of the GDPR into question, a controller that documents a genuine or potential conflict with third-country law and seeks in good faith to reconcile it is in a different position from one that disregards the GDPR. Ignoring this difference would penalise precisely the European companies that compete globally.

We propose adding the following at the end of paragraph 107:

"The legal context includes situations where supervisory authorities have adopted diverging positions on the interpretation of the provision concerned, including in cross-border cases, and no EDPB guidance addresses the matter. In such situations, the supervisory authority should take into account, as a mitigating factor, that the controller or processor acted in accordance with the published position of a supervisory authority. The legal context also includes situations where the controller or processor, operating across jurisdictions, is subject to obligations under the law of a third country that conflict, or might potentially conflict, with its obligations under the GDPR. Without prejudice to Article 48 of the GDPR, where the controller or processor has assessed and documented such a conflict or a potential conflict, has sought in good faith to reconcile those obligations, and has adopted the least intrusive measures for data subjects, the supervisory authority should take this into account as a mitigating factor. In both situations, the supervisory

authority should consider whether an order pursuant to Article 58(2)(d) of the GDPR is the most appropriate response."

We also propose adding the following at the end of paragraph 72:

"A controller or processor that has aligned its conduct with the published position of a supervisory authority on the matter concerned should, as a rule, be considered to have acted with a low degree of negligence."

### Remediation, including after acquisitions

Corporate transactions are frequent in the digital sector, and they are often an opportunity to raise the level of data protection. An acquirer may take over a product or service built with less mature compliance practices, or outside the GDPR framework, and bring it up to the requisite standard. This is a positive outcome for data subjects, and enforcement should encourage it. Nevertheless, a change of control does not reset the compliance history and relevant responsibility or create a grace period for compliance. Accordingly, we fully agree that acquirers should carry out appropriate due diligence and take prompt, documented steps to address any compliance gaps identified. Where they do so, the Draft Guidelines should recognise it when weighing previous infringements, when assessing mitigating measures, and, above all, when deciding whether a fine is necessary, as set out below:

- **Previous infringements**. Article 83(2)(e) of the GDPR aims to assess the controller's attitude towards compliance. A change of control does not erase previous infringements, but documented changes in governance and controls should be recognised as a mitigating factor.

  We propose inserting the following new paragraph after paragraph 87:

  "Where the controller or processor has been subject to a change of control, the supervisory authority should take into account prompt and documented measures taken following that change to address a previous infringement. Such an infringement may carry limited weight as an indication of the current attitude of the controller or processor towards compliance, in particular where, following the change of control, prompt and documented measures have been taken to address the matter concerned."

- **Remediation as mitigation**. Paragraph 74 gives particular weight to measures implemented spontaneously, before the investigation becomes known to the controller. Remediation following an acquisition, driven by the acquirer's own due diligence, is a clear example.

  We propose adding the following at the end of paragraph 74:

"This includes measures adopted by a controller or processor, following a change of control, to address compliance gaps identified through its own due diligence or review, where those measures were adopted before the commencement of the supervisory authority's investigation."

- **Whether a fine is necessary**. Administrative fines have a punitive and deterrent function (paragraphs 18 and 112). Where a controller has, following a change of control, ended an infringement and prevented its recurrence, specific deterrence has already been achieved. Imposing a fine in the same way as on a controller that persisted in the infringement would also weaken the incentive to remedy infringements promptly, which is what protects data subjects the most. The Draft Guidelines already recognise, in line with Land Hessen (C-768/21), that a supervisory authority may refrain from taking a corrective measure where the controller, as soon as it became aware of an infringement, has brought it to an end and ensured it does not recur (paragraph 117).

  We propose adding the following at the end of paragraph 117:

  "This may be the case, in particular, where an infringement originated before a change of control of the controller or processor and, following that change, the controller or processor has promptly brought the infringement to an end and adopted documented measures to prevent its recurrence. In such cases, the supervisory authority should consider whether an administrative fine is necessary to achieve its objectives, taking into account that discouraging the remediation of acquired products and services would not serve the protection of data subjects."

  We also propose adding the following example to Section 5.3.2:

  "Example: Remediation following an acquisition. A company operating an online service undergoes a change of control and remains the controller of the relevant processing. During its post-acquisition review, the controller identifies that the service retained inactive user accounts indefinitely, without a defined retention period. Within six months of the acquisition, and before any complaint, the controller defines a retention policy, deletes the accounts concerned, and updates its transparency information. A complaint subsequently submitted to the supervisory authority concerns the period before the remediation. The supervisory authority finds an infringement of Article 5(1)(e) of the GDPR. Having assessed the relevant factors under Article 83(2) of the GDPR, it considers the infringement minor in the particular circumstances of the case. Taking into account that the controller brought the infringement to an end promptly and through its own initiative, and that it has adopted documented measures to prevent its recurrence, the supervisory authority finds that an administrative fine would not be necessary or proportionate and that no further corrective measure is necessary or proportionate, and therefore decides not to exercise further corrective powers."

# Conclusion

The Draft Guidelines are an important step towards a more consistent enforcement of the GDPR across the EEA. A shared methodology for deciding when a fine is appropriate benefits supervisory authorities, organisations, and data subjects alike.

To achieve this, the final Guidelines should properly weigh how controllers actually behave: the diligence they exercise, the measures they invest in, and the steps they take to remedy shortcomings, including in products they acquire. Enforcement that clearly recognises these efforts encourages organisations to invest in the measures that protect individuals most. When rules are predictable and applied consistently across Member States, they are easier to comply with and more effective in practice.

Bending Spoons appreciates the opportunity to contribute to this consultation and remains available for further discussion on any of the points above.