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

**Response from GeoTapp**
Submitted by Michele Angelo Petraroli, founder, GeoTapp
Public consultation open 21 September to 13 November 2026

## About this response

GeoTapp develops a time tracking application for companies whose teams work away from a fixed office: cleaning contractors, security firms, construction and trades, maintenance and installation businesses. The company is established in Italy and is a micro business. It offers the product across Europe, in eleven languages.

Two things are declared at the outset, because both affect how much weight this response deserves.

The first is that the product is young and the installed base is small. Where this response describes what employers do or believe, it describes the questions buyers ask before they buy and the configurations they ask for, not a survey. Nothing here should be read as evidence of how common a practice is.

The second is that the product was deliberately built so that it cannot follow a worker through the day. Location is recorded when a shift is opened and when it is closed, the worker sees both records on a map inside their own app, and nothing is recorded in between. That is a design constraint rather than a setting an administrator can turn up. It is verifiable without asking us: the Android package does not request background location and runs no foreground location service, and on iOS the app asks only for when in use authorisation and stops location updates at the first fix. This matters for one reason only, which is that it makes us an interested party. Several comments below would raise the cost of the more intrusive configurations that competing products offer and we chose not to build. The consultation should weigh them in that light.

This response does not comment on the Calculation Guidelines, on the legal preconditions in steps 1 to 3, or on the treatment of public authorities. It comments on one thing: how the methodology in steps 4 and 5 will land on small employers who monitor people at work, because that is the only subject on which we see anything the EDPB cannot see more clearly from where it sits.

## 1. The guidelines do not reach the employment context, and that is where small controllers most often meet Article 83

Two observations about the text as adopted on 17 September 2026.

Article 88 GDPR, the provision that exists specifically for processing in the employment context and under which most Member States have adopted national rules, is not cited anywhere in the document. The word "location" does not appear either.

The employment context is not entirely absent. Example 1 concerns an AI system analysing employee communications for productivity assessment, and Example 11 concerns unlawful access by an employee to customer data. But Example 1 is there to illustrate a controller who proceeds despite a warning, and Example 11 concerns an employee as the source of the breach rather than as the person whose data is processed. None of the fourteen examples shows an ordinary workplace monitoring case being assessed under step 4.

That is a gap worth closing, because the population of controllers who will read these guidelines most carefully is not made of large technology companies. It is made of the fifteen person cleaning contractor whose supervisory authority has just written to it about the app on its staff's phones. The guidelines are otherwise attentive to that population: "SME" appears forty five times, Examples 6 and 7 are expressly about SMEs, and Example 9 concerns a small sports club.

**Suggestion.** Add one worked example in Section 5.2.13 drawn from ordinary workplace monitoring by a small employer, and add a reference to Article 88 GDPR and to national employment rules among the factors relevant to Article 83(2)(a) and (d). The supervisory authorities have ample decided cases to draw an example from.

---

## 2. Article 83(2)(d): the controller often cannot know what the tool records, and Example 7 already says so

Paragraphs 75 to 77 ask the supervisory authority to assess whether the controller "did what it could be expected to do" given the nature, purposes and size of the processing.

For a ten person company that bought an off the shelf application, what it can be expected to do is bounded by what the supplier told it the product does. Small employers do not read manifests. They do not know at what interval a position is sampled, whether the sampling continues after the shift is closed, or whether an administrator console exposes a live map. In our experience the buyer discovers these properties after purchase, and sometimes only when a worker complains.

The guidelines already contain this reasoning, in Example 7: an SME was found to have infringed Article 32(1) because a function activated in a social media provider's developer tool took precedence over the settings the organisation had configured in its own platform, and the supervisory authority treated the infringement as minor. The supplier's behaviour was decisive to the outcome, but it is presented as a fact of that case rather than as a factor with a name.

**Suggestion.** State expressly under Article 83(2)(d) that where processing is carried out through a third party product, the supervisory authority may take into account what the supplier declared in writing about the product's behaviour: what it records, at what frequency, under what conditions it records nothing, and what it is technically incapable of doing. Where the product behaved differently from what was declared, that should weigh in mitigation for the controller. Where the capability was declared and the controller chose to enable it, it should weigh the other way, and the declaration removes the defence that the controller did not know.

We note that this proposal places a burden on suppliers, and we are one. It would require us to state in writing what our product records, and to be held to it. We think that is the right allocation, because the

supplier is the only party in the chain that knows the answer without having to investigate.

## 3. Article 83(2)(a): where processing observes people over time, gravity sits in the configuration

Section 5.2.2 treats nature, gravity and duration largely through the scope of the processing and the number of data subjects affected. In workplace monitoring, those are poor proxies.

The clearest recent illustration is the Italian supervisory authority's decision no. 382 of 28 May 2026 concerning a regional health authority. Position was recorded from company vehicles every sixty seconds. The Garante described the result as systematic monitoring of employees' movements and as pervasive processing, and stated that where the periodicity of collection is extremely close, as it was in that case, it conflicts with the general principles. The number of people affected was modest and the fine was six thousand euro. What made the processing grave was not the headcount. It was the interval, the fact that a real time access function was available, and the absence of a prior impact assessment. The measure that changed the situation was the move to a fifteen minute interval and the disabling of real time access.

**Suggestion.** Add to Section 5.2.2 that where the processing consists in the observation of identified individuals over time, the assessment of gravity should consider the sampling frequency, whether recording continues outside the period the processing was justified for, and whether the person observed can see what has been recorded about them. These three properties are objectively verifiable from the product itself, they do not depend on the controller's account of its own intentions, and they discriminate between configurations far better than the number of data subjects does.

## 4. Section 3.5: in continuing configurations, the order is the measure that stops the harm

Paragraphs 27 to 29 describe the orders under Article 58(2), including the order under Article 58(2)(d) to bring processing into compliance within a specified period.

Workplace monitoring infringements are rarely events. They are settings, and the setting keeps running while the procedure is pending and after it concludes. A fine imposed on a controller whose configuration is left untouched produces a controller that has paid and is still recording.

**Suggestion, two parts.** First, state that where the infringement consists in a processing configuration that continues to operate, an order under Article 58(2)(d), with a specified period, should accompany whichever measure is selected at step 5, including where the infringement is found minor and a reprimand is issued under step 5 a. Otherwise the outcome of the minor track is an acknowledgement that changes nothing.

Second, address the data already collected. Where a configuration is found unlawful, the personal data it produced remains in the controller's systems and remains available for use against the individuals it describes, in a disciplinary procedure or in litigation. Erasure under Article 58(2)(g) is listed in paragraph 28 but the guidelines do not discuss when it should follow a finding. In our sector this is the remedy that

changes behaviour, more than the amount of any fine, because it removes the reason the excessive configuration was chosen.

## 5. Paragraph 120: the "disproportionate burden" passage will be read as "small companies are not fined"

Paragraph 120 states that a supervisory authority may choose a reprimand instead of a fine where the fine likely to be imposed for an infringement not considered minor would constitute a disproportionate burden on a natural or legal person.

The principle is sound. The reading it will receive in our market is not. The belief we meet most often when a buyer asks whether a configuration is lawful is that first offences produce a letter, and that a company of fifteen people is too small to be fined. Paragraph 120, quoted without its context, will be offered as authority for that belief within days of the final version being published, and it will be quoted by the suppliers whose products record the most.

**Suggestion.** State expressly that the size of the controller does not by itself make a fine disproportionate, and that the disproportionate burden assessment concerns the effect of the amount in the individual case rather than the category of controller. And pair it with the point above: where a reprimand is issued under paragraph 120 for an infringement that is not minor, an order to bring the processing into compliance should ordinarily accompany it, so that the outcome is not both no fine and no change.

## 6. On the presumption itself

The methodology in step 5 b, under which an infringement that is not minor will as a general rule attract a fine, is in our view the most consequential part of the document, and we support it.

The reason we give is commercial rather than moral, and we state it plainly because the consultation is better served by an honest interest than by a principle we do not have to pay for. Where the expected outcome of an unlawful monitoring configuration is a reprimand, the supplier that records more has an advantage, because the restraint built into a more limited product costs real engineering and returns nothing to the buyer. A buyer choosing between two applications is choosing between more data and less data at the same price, with no downside attached to the first. The presumption in step 5 b attaches a cost to the first, and that cost is what makes the second saleable.

We would add one caution about paragraph 119. The discretion it preserves is necessary, but the combination of a general rule in paragraph 119 and a broad exception in paragraph 120 leaves the outcome hard to predict for exactly the controllers who most need to predict it. If the EDPB can say in the final version what a supervisory authority should record when it departs from the general rule, the presumption will do more work than the rule alone.

## What this response does not say

It does not ask for a lighter regime for small controllers. The proposals above increase what is expected of small employers who monitor people, by removing the defence of not having asked what their software does, and increase what is expected of their suppliers, including us.

It does not comment on the calculation of amounts, which is the subject of the Calculation Guidelines, nor on the interplay with the Digital Services Act addressed in the guidelines adopted at the same plenary.

---

## Sources cited


- 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 17 September 2026: https://www.edpb.europa.eu/documents/guideline/guidelines-042026-on-the-application-of-the-power-to-impose-administrative_en
- Garante per la protezione dei dati personali, provvedimento no. 382 of 28 May 2026, doc. web 10259916: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10259916