Draft guidelines on the power of data protection authorities to impose administrative fines

by Bruno RASLE – bruno_rasle@halte-au-spam.com *Paris, 11th November 2026*

On 17 September 2026, the EDPS adopted a draft of guidelines on the power to impose sanctions and other corrective measures by data protection authorities under the GDPR. This draft is subject to a public consultation.

The EDPS states that this draft guidelines, relating to the full taxation those ' relating to the calculation ' 04/2022 adopted on 24 May 2023 are intended to supplement the guidelines on the methodology to be followed when determining the amount of an administrative fine.

The EDPS also states that, once approved, these new guidelines replace those of the WP29 concerning the application and setting of administrative fines under Regulation 2016/679 (WP253) adopted on 3 October 2017.

My main proposal focuses on the DPO: **A chapter dedicated to the Data Protection Officer should be added**

Unfortunately, it has been observed that, on many occasions, the recommendations of DPOs are not heeded by the organisations that appointed them, whether in the context of data processing projects or in the event of data breaches (it is very common for the data controller to fail to notify the supervisory authority even when the circumstances require them to do so, despite the advice of the Data Protection Officer). If, indeed, the DPO is the key factor in ensuring compliance with the GDPR (and thus in reducing the number of cases where it is necessary to impose a sanction), this element of self-regulation should be incorporated into the draft.

It is regrettable that the draft only mentions the DPO two instances and only to a minor extent:

- in paragraph 78 ('*In order to adequately assess the above elements, the supervisory authority should take into account … whether there has been contact with the Data Protection Officer or data subjects (if applicable).*");
- paragraph 85 suggests that, for a data controller, knowingly disregarding the advice of their DPO constitutes an aggravating circumstance ('*For example, this would be the case for infringements arising as a consequence of having ignored the advice of the Data Protection Officer").*

At the very least, something much clearer would be needed, as is the case in the Guideline 04/2022 on the calculation of administrative fines under the GDPR, which includes the following passages:

- "*The telephone company did this despite advice against it from the data protection officer...*";
- "*The seriousness of the infringement was increased, however, by the fact that the infringement was committed in contrary to an advice from the data protection officer and, thus, considered intentional*";
- "*For example, this would be the case for infringements arising as a consequence of having ignored the advice provided by the Data Protection Officer*".

Similarly, on page 12 of WP 253, which the draft is intended to replace, the following passage appears: "*Circumstances indicative of intentional breaches might be unlawful processing authorised explicitly by the top management hierarchy of the controller, or in spite of advice from the data protection officer or in disregard for existing policies".* To strengthen the role of data protection officers, it should be clarified that such a scenario – given its intentional nature – could not be regarded as constituting a minor breach.

During the hearing phase, which allows the organisation facing the risk of a sanction under the GDPR, the draft should also specify what the supervisory authorities expect of DPOs. Thus, at the conference held on 29 September 2026 by the CNIL, in response to a question I put to the Chair of the select panel (responsible in France for deciding on sanctions, their nature and their amount where they take the form of a fine), I was given the following response in essence: "*As regards DPOs, we pay close attention to their role. They are our ambassadors within organisations. When you look at certain sanctions, you will notice that they are more severe, harsher, because the DPO had warned the organisation but was not listened to. When the DPO fulfils their role, we know it. Similarly, during a hearing before the DPA, [if] the DPO has been « brought » as if one were bringing in a palm tree, we are also sensitive to this as well.*'. The recording is available here (My question and the response from the Chair of the committee can be found at the very end of the conference). It is essential that these rules be adopted by all DPAs and clearly set out in the guidelines, so that they are formalised and known to all.

Conversely, it would be worth clarifying that the fact that a data controller has taken care to seek the opinion of their DPO and to act on it is interpreted as a sign of goodwill, as the Garante noted in case 9440025 of 2 July 2020 (The penalty that was initially envisaged has been reduced).

Having made it clear that knowingly disregarding the advice of its DPO (for example, by failing to report a data breach) is an aggravating circumstance, the chapter devoted to this role could include other points:

- Paragraph 49 of the draft contains the following passage: '*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. 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.*". Furthermore, paragraph 50 states that "*However, where EDPB Guidelines exist, an error is always to be considered avoidable and therefore at least negligent.*'. Here, an explicit link should be made to the obligation on organisations that have appointed a DPO to enable them to maintain their specialist knowledge (Article 38(2) of the GDPR), as it is the DPO's responsibility to carry out the monitoring implied in these two points;

- Point 78 should be clarified. In its current wording ('*...whether there has been contact with the Data Protection Officer ...*'), it is unclear who initiated this contact. If – as is assumed – the data controller, it would be advisable to state this explicitly. The guidelines could encourage organisations to keep a record of the views expressed by their DPO to them as well as their formal exchanges and meetings, as stated by the Italian Data Protection Authority in its decision 9440025 of 2 July 2020 ;

- It should be clarified whether the voluntary appointment of a DPO is taken into account (and, if so, in what way) in the decision to impose a sanction.

All these points could give greater weight to the role of the DPO and increase the likelihood of achieving a high level of compliance with the GDPR organisations. Nevertheless, the fact that a dedicated chapter has been created for the DPO in no way precludes mentioning the DPO elsewhere in the draft, whenever this is relevant and in line with the objectives of the draft guidelines.

I would also like to make the following proposals and comments regarding this draft:

1. Point 1. states that that these new guidelines are intended to ensure the consistent application of the GDPR. Does this mean that, under the same circumstances, the same breach would be penalised in exactly the same way throughout the European Union, which would prevent *'forum shopping'*? However, it is said that the supervisory authorities would also take into account the economic standing of each Member State. If this is not an unfounded rumour, this should be clarified in the guidelines;

2. And is this intended uniformity merely geographical, or does it also apply over time? May the same breach be penalised differently over time, and if so, according to what criteria?

3. Point 21 deals with warnings, which, in France, are not sanctions. The guidelines should specify whether such warnings may (or not) be made public, and if so, what the objectives of such publication are and what rules the supervisory authorities would follow would follow in making that decision;

4. Point 26 refers to the possibility for supervisory authorities to issue a reprimand where local law prevents prevent them from imposing a financial penalty. It would be useful for the guidelines to list the Member States concerned by a provision of this nature;

5. Paragraph 3 of point 28 reiterates the power of supervisory authorities to require a data controller to notify data subjects of a data breach affected. When such a power is exercised, it would be advisable for the authority to clearly indicate the reasoning it followed in reaching the conclusion that the breach was likely to pose a high risk to those individuals (and not merely a list of the factors taken into account, but rather a description of a documented, explainable and reproducible method that was followed). Furthermore, is it reasonable for a data controller to be sanctioned for failing to notify a data breach to the data subjects, when the supervisory authority did not specify this requirement upon receiving the notification (in which the data controller clearly set out the reasoning behind their decision not to make such a notification)?

6. Section 4.3 provides for only two situations, depending on whether the breach was committed knowingly (intentionally) or through negligence. Is there not a third possibility missing, for example where a data breach has been perpetrated by a hacker exploiting a *zero-day* even though the organisation had fully complied with state-of-the-art security standards? What about situations where the data subject puts themselves at risk, for example by failing to protect their passwords adequately? The guidelines should also address these situations.

7. Point 50 addresses the fact that a data controller cannot hide behind their ignorance of the GDPR or the guidance published by the EDPB to justify a breach. Does this rule also apply to the guidance additionally published by each supervisory authority (which may go beyond that of the EDPB)? If so (as numerous penalty decisions demonstrate), the guidelines should have been clarified on this point.

8. Point 58 deals with the deterrent nature of the sanction imposed. It would be advisable to specify towards whom this deterrent effect is intended. Is the aim to deter the sanctioned organisation from repeating its infringements? The same infringements? Or, particularly where the sanction is publicised, to deter other organisations from committing the same infringements?

9. Among the criteria listed in paragraph 64 for determining the seriousness of the breach is the number of data subjects affected. It should be noted that this criterion does not appear in the EDPB guidelines on the notification of data breaches (which, if likely to pose a risk to even a

single data subject, must be reported to the supervisory authority). This lack of clarity could lead to misunderstandings.

10. Paragraph 70 states that the duration of the breach is taken into account. Should this not be included in the section where negligence is assessed?

11. Point 72 introduces the concepts of 'low-level' and 'high-level' negligence. It would be useful to clarify these concepts and provide concrete examples. Are these the examples provided in section 5.2.13?

12. Paragraph 73 states that the fact of taking immediate, concrete measures to mitigate the consequences of the breaches for those affected – and not merely to achieve compliance – is a mitigating factor. Here again, it would be useful to provide concrete examples of such measures.

13. Paragraph 79 states that '*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.* '. It should be added that decisions which are the subject of an appeal may under no circumstances be taken into account.

14. Paragraph 82 states that "*Some national laws impose an obligation to delete data after a certain period, which prevents the competent supervisory authority from taking these precedents into account.* ". It should be added that, conversely, supervisory authorities may take into account sanction decisions that have been anonymised (as is the case in France, two years after their publication), to avoid any ambiguity.

15. Point 91 refers to '*exceptional efforts*' that might be undertaken by an organisation and which supervisory authorities could take into account in their decision on sanctions. Here again, to help DPOs to promote the implementation of these exceptional efforts, it would be helpful to provide some concrete examples.

16. Point 113 states that '*Where there is a choice between several (equally) appropriate penalties, to the supervisory authority should impose the one which is the least onerous.*'. This sentence needs clarification and further detail. During the adversarial phase, the defence often acknowledges the breaches but calls for a different or less severe sanction. Here too, concrete examples would help to better understand this provision.

17. On page 13, the draft provides an example of a measure taken by a data controller to try to compensate for the inconvenience caused to a data subject by processing. It would be useful to provide further concrete examples.

Finally, it would be helpful if the guidelines clarified these other points, which are absent from the draft:

18. The draft makes no mention of sanctions imposed in cases where a data processor is a party to the processing and in situations of joint controllers. What rules do supervisory authorities follow in such cases to determine which organisation is liable to be sanctioned? (These rules should be illustrated with concrete examples.). Can be 'allocate' a penalty amongst several of these parties, and if so, according to which rules? Could this be seen as a decision to publicity for one of the joint data controllers but not for others? In the event of joint controllers, if one of the parties appeals against the decision to impose a sanction, is that decision also called into question for the other joint controllers?

19. Some providers of certified training courses and certification bodies claim that the fact being certified is regarded by the authorities as a mitigating factor, which seems shocking to say the least (on the contrary, a certified body found to be in breach should, at the very least, have its certification withdrawn). Are these commercial arguments actually supported by the supervisory authorities and the EDPB? The chapter dealing with certification is silent on this matter. The guidelines were intended to clarify this point.

Bruno Rasle describes himself as a 'monomaniac' when it comes to GDPR compliance and practises this 'martial art' in three ways: professionally, he has served as a shared data protection officer for one of the branches of the French Social Security, appointed to oversee more than a hundred data controllers; on a voluntary basis, he is one of the very first members of the AFCDP (association bringing together professionals in the *Privacy* in France) and served as its general delegate for around twelve years; finally, as a lecturer, he teaches on the oldest and most advanced course in Europe (he trains *Privacy* since 2007). He also played an active role in establishing the role of Data Protection Officer. He is co-author of the following books: *Stop Spam* (Eyrolles, 2003); *Data Protection Officer: Much More Than a profession* (AFCDP, 2015); *The Right to be Forgotten* (Larcier, 2015); *Preparing for the GDPR* (Éditions législatives, 2017). He founded the AFCDP University for DPOs, the *AFCDP Index of the Right of Access*, and the *DPO Job Board* for DPOs and the *Code of Ethics* for DPOs. He helped to establish CEDPO (European Confederation of Associations of Privacy Professionals), of which he was a *board member*. He has authored numerous publications, including ' *GDPR Impact Assessment: should it be illustrated with a risk matrix, and if so, which one?* ", " *The DPO: a source of discomfort or a creator of value?* ", " *Notifying victims of a data breach: going beyond the GDPR?* " or " *We must save Private DPO!* ". In addition to his teaching on the Specialised Master's programme in '*Management and Personal Data Protection*' at ISEP, the DPO Master's at Oteria and the DPO University Diploma at Panthéon-Assas, he also delivers short training courses on behalf of Anaxia Conseil.