Step 2: who can be fined

- **Allocation of responsibility.** The final Guidelines should confirm that a controller or processor may be fined only for a breach of obligations addressed to it. Paragraph 42 describes Article 28 as addressed to processors, but Article 28(3) requires the controller to put a compliant contract in place. Without this clarification, a processor could be fined for a failing that the GDPR places on the controller. Article 82(2) draws the same line for compensation. (See paras. 40 and 42.)
- **Change of role under Article 28(10).** Paragraph 42 states that a processor becomes a separate controller where it departs from the framework or detailed arrangements set by the controller. However, Article 28(10) applies only where the processor itself determines the purposes and means of processing. The final Guidelines should confirm that an unintended technical deviation, such as a software error, is not, on its own, enough to change the parties' roles. Clear criteria would give both controllers and processors certainty about where responsibility lies. (See para. 42.)
- **Separate liability for others' misconduct.** Consistent with NVSC, C-683/21, a controller should incur separate liability, for example under Article 32, only where it has culpably failed to meet an identifiable obligation. A rogue act by a processor or employee shows that something went wrong, not that the controller's precautions were deficient. Treating the act itself as proof would bypass the attribution limits set in NVSC. (See paras. 42 and 43.)
- **Group liability.** Paragraph 45 accepts national rules that make a parent company liable to pay a fine. The final Guidelines should confirm that these rules concern recovery of the fine only. They should not make a parent or other group company liable for the infringement itself, which must still be established against the addressee under Steps 1 to 3. (See para. 45.)

Step 3: intent and negligence

- **Effect of existing EDPB guidance.** Paragraph 49 asks only whether the organisation was in a position to know its conduct was unlawful, and the final sentence of paragraph 50 treats any error as avoidable wherever EDPB guidelines exist. Combined, these leave little room for a finding of no fault. The final sentence of paragraph 50 should be removed. Failing that, it should cover only adopted guidelines that pre-date the conduct and deal specifically with the point in question. EDPB guidelines do not bind controllers or processors, and their wording is often open to differing interpretations. Their existence cannot therefore settle whether an error could reasonably have been avoided. The burden should remain on the authority to prove negligence by reference to the evidence in the particular case. (See paras. 49 and 50.)
- **Reliance on reasoned legal advice.** An organisation that can show it analysed the question carefully, including the arguments against its position, should be treated as less culpable. Example 4 rules out reliance on advice simply because it reaches a minority conclusion or differs from what an authority is thought to prefer. That approach rewards organisations that avoid difficult questions, contrary to the spirit of Article 5(2). A deliberate decision to accept legal risk is different from acting where the legal position is truly open, for instance on new technologies or where national authorities have taken inconsistent approaches. As Examples 9 and 14 already suggest, the latter should point to a lower degree of negligence at Step 4. Organisations should be able to show they acted diligently while keeping their legal advice protected, yet Example 4(c) gives no weight to advice that is not provided to the authority. (See paras. 50, 71 and 72 and Examples 4, 9 and 14.)

Step 4: minor infringements and the Article 83(2) factors

- **Scale and organisational size.** The breadth of the processing, how widespread the issue was and the population “potentially affected” should be measured by reference to the specific failure, looking at what damage, or real likelihood of damage, resulted. Otherwise, these factors will weigh against large organisations in almost every case. An infringement by a large organisation can still be minor. Almost all the current examples concern SMEs. Illustrations involving larger organisations, such as a short-lived disclosure to the wrong recipient that was contained at once, or a retention schedule applied late

to a small set of records, would show how the minor category applies to them. (See paras. 56 and 66 to 69 and Examples 6 to 10.)

- **Purpose-related risk.** Paragraph 65 already recognises that the role of the controller or processor is relevant. Risks that flow from the purpose of the processing, such as monitoring or profiling, should be attributed to the party that determined that purpose. The “core activities” factor in paragraph 67 should be applied on the same basis, so that it reflects each party's actual role rather than the nature of its business. (See paras. 65 and 67.)
- **Duration.** Paragraph 70 treats a longer infringement as more serious. Duration should run from the point at which the unlawfulness of the conduct became reasonably apparent, for example after a relevant CJEU ruling or final guidance, rather than from when the processing began. (See para. 70.)
- **Mitigating factors.** Robust technical and organisational measures, swift corrective action, a cooperative approach to the investigation and full compliance with any earlier orders should be capable of mitigating without the organisation having to go “above and beyond” its obligations. Article 83(2)(d) expressly requires account to be taken of measures adopted under Articles 24, 25 and 32. As drafted, weak measures aggravate but strong measures are at best neutral, which reduces the incentive to invest in compliance. (See paras. 75 to 77, 90, 91 and 99.)
- **Previous infringements.** Paragraphs 80 and 87 allow any earlier infringement to aggravate, regardless of its subject matter or the authority that made the finding. Paragraph 82 also rejects any fixed time limit. Only infringements by the same entity, acting in the same role, on a relevant subject matter should count, as unrelated findings say little about the infringement under review. A clear look-back period, for example five years, would give certainty and support consistency across Member States. Conversely, an unblemished compliance history over a sustained period should be capable of counting in the organisation's favour. (See paras. 80 to 88.)
- **Effect of an earlier reprimand.** Example 5 suggests that a reprimand for a minor infringement can make a later similar infringement non-minor. The final Guidelines should confirm that an earlier reprimand is one factor to weigh, not a reason in itself to move to a fine, particularly where the organisation has since taken remedial steps. (See para. 88 and Example 5.)
- **Notification and support beyond the legal minimum.** The draft treats mandatory notification as neutral. Where any party in the processing chain shares information about an incident more fully than the law requires, or actively supports another party's response, this should be capable of mitigating, as it helps limit harm to data subjects. (See paras. 73, 74, 95 and 96.)
- **Codes of conduct and certification.** Article 83(2)(j) covers both, but section 5.2.11 says little about certification and treats adherence mainly as a reason not to add further measures. Adherence should be capable of mitigating in its own right, to encourage participation in approved schemes. (See paras. 101 to 104.)
- **Economic gain.** Paragraphs 106 and 107 treat profit obtained or losses avoided as a strong indicator that a fine is needed. The final Guidelines should confirm that only gain caused by the infringement counts, not ordinary revenue from the service concerned that would have been earned anyway. (See paras. 106 and 107.)

Step 5: choice of measure

- **Presumption in favour of fines.** The “strong presumption” of a fine for non-minor infringements should be replaced with neutral wording, such as “a fine will normally be the appropriate measure, subject to a full assessment of the specific case”. Under Article 83(2) and Land Hessen, C-768/21, the measure chosen must be tailored to the facts, and a presumption risks displacing that assessment. Worked examples would help show where a non-minor infringement still calls only for a reprimand or an order under Article 58(2), for instance a first breach by an organisation that acted on a defensible reading of the law and has since changed its practice. (See paras. 57, 119 and 120 and Example 14.)
- **General deterrence.** Paragraph 112 states that supervisory authorities should maintain a practice of imposing fines to deter others. General deterrence is a legitimate aim, but it should not justify a fine that is disproportionate on the facts of the individual case. (See paras. 112 and 113.)

- **Overlapping regimes.** The draft accepts that GDPR fines are criminal in nature for Charter purposes, so Article 50 of the Charter applies. Supervisory authorities should therefore coordinate with and take account of penalties imposed for the same conduct under other EU regimes, such as the AI Act, consistent with bpost, C-117/20. (See para. 100 and footnote 8.)
- **Reasons.** Paragraph 12 recognises the duty to give reasons, but paragraph 10 permits authorities to omit reasons on aspects considered inapplicable. Supervisory authorities should explain why the chosen measure is necessary and proportionate, including why a less onerous measure would not suffice. A factor relied on at Step 4 should also not be counted again as aggravating when the fine is calculated. (See paras. 10, 12, 61 and 113.)
- **Right to be heard on the measure.** Paragraph 60 notes that, under some national rules, a lead authority's draft decision may contain limited detail on the sanction. Organisations should still have an opportunity to comment on the proposed corrective measure and the factors on which the authority relies before a final decision is taken, including in cross-border cases. (See paras. 3 and 60.)