1 Background

1.1 This document sets out the formal response of DLA Piper UK LLP ("**DLA Piper**" or "**we**") to the Information Commissioner's Office ("**ICO**") consultation on its draft guidance about how it decides to issue penalty notices and calculate fines under the UK General Data Protection Regulation ("**UK GDPR**") and Data Protection Act 2018 ("**DPA 2018**")[1].

1.2 DLA Piper is a global law firm and has one of the largest international cyber security and data protection teams in the world[2]. It advises lots of clients across lots of different regions and so has a broader and global perspective of data protection law and its impact on commerce.

1.3 This document sets out the views of the firm and not the formal position of any one person or any of the firm's clients. DLA Piper consents to the ICO publishing its name and its response.

1.4 The headings and questions set out below mirror those published by the ICO in its consultation to the guidance, to make it easier for the ICO to collate and consider all responses that it receives.

2 Statutory background

Do you have any comments on our approach to the concept of an 'undertaking' for the purpose of imposing fines?

2.1 Reference to "undertaking" in this context is widely recognised in competition law and is also referred to in the General Data Protection Regulation ("**GDPR**") itself. It is therefore logical for it to be referred to in this way in the draft guidance.

2.2 While deviation from this reference could create unnecessary ambiguity in interpretation between the UK and EU, we feel that a greater level of definition could be provided.

2.3 A controller or processor under consideration for a penalty under the GDPR is likely to be an undertaking personified through a legal entity, rather than a self-employed worker or a professional. Legal entities can be configured in different ways[3]:

(a) Standalone legal entities – economic entities that may be run by a standalone legal entity. In this scenario, the undertaking and the legal entity are, in effect, the same. In the event of enforcement by the ICO, the legal entity would appear as the corporate body that personifies the undertaking.

(b) Groups of companies under sole control – legal entities may control other entities that are legally separate. These can be referred to as "affiliates" or "subsidiaries," with the entity in control referred to as the "parent company".

---

[1] https://ico.org.uk/about-the-ico/what-we-do/draft-data-protection-fining-guidance/

[2] By way of example, the firm maintains a popular online resource called DLA Piper, Data Protection Laws of the World which sets out key features of data protection laws from around the world upon which the firm can advise. The most recent version of the resource includes the data protection law for over 150 different jurisdictions.

[3] Araujo Boyd, Marcos (2023) The notion of undertaking in EU competition law.

2.4 Enforcement by the ICO against an undertaking in the form of a standalone legal entity is clear and justifiable. The position is more complicated with respect to enforcing against an undertaking in the form of groups of companies under sole control.

2.5 It may initially be understood that a group of companies as defined should be considered for all purposes under competition law as an undertaking. That perspective is followed in the field of merger control: under the EU Merger Regulation[4], all the entities under the control of an 'undertaking concerned' are assumed to be a part of it both for the purposes of turnover calculation.

2.6 It is usual in other penalty setting regimes in the UK for the sentencing authority to limit their consideration for the purposes of penalty to the offending entity. We agree that a more just outcome is obtained where comprehensive financial information is provided, enabling the penalty setter to make an accurate assessment of financial status. Normally only information about the offender should be relevant. It is only where fairness allows that the resources of a linked organisation can be properly taken into account, where for example the resources of that linked organisation are available to the offender.

2.7 This reference to an "undertaking," for the purposes of turnover calculation in the context of penalties under the GDPR, however, requires a more detailed analysis in order that a just outcome is achieved.

2.8 The Court in *ICI v European Commission*[5] considered this and linking the issue of treating subsidiaries as part of an undertaking to their lack of autonomy. It concluded that economic unity would require:

> *"… that the subsidiary, although having separate legal personality, does not decide independently upon its own conduct on the market, but carries out, in all material respects, the instructions given to it by the parent company."*

2.9 This reference to an "undertaking" for the purposes of turnover calculation in the context of penalties under the GDPR, however, requires a more detailed analysis in order that a just outcome is achieved.

2.10 The key and equitable outcome when referring to turnover when imposing penalties would be with reference to the decision maker of the entity in question, which is a more nuanced analysis than simply the groups of companies under sole control. Imposing a penalty based on turnover of the undertaking may not necessarily lead to a proportionate or justifiable outcome.

Do you have any comments on our approach to fines where there is more than one infringement by an organisation?

2.11 The guidance contains or implies an internal contradiction: it both states that the ICO:

(a) will consider the imposition of separate penalties where the conduct is not part of 'the same or linked processing operations' that will each apply separately and in an additive form and, while each penalty independently cannot exceed the statutory maximum, the total penalty imposed may, in aggregate, exceed that sum[6]; and

[4] The Merger Regulation, Council Reg. (EC) 139/2004 (OJ 2004 L24/1, 29/1/2004).

[5] Imperial Chemical Industries v Commission of the European Communities, 48/69, ECLI:EU:C:1972:70 at 133

[6] Paragraphs 23 to 29 of the Guidance

(b) will limit the totality of the penalty set, once aggregated, to the statutory maximum for the most serious infringement[7], where the organisation's overall conduct has infringed more than one provision of the legislation[8].

2.12 The correct interpretation of Article 83(3) is that the "total amount" that can be imposed relates to all infringements being considered in aggregate and effectively limited to the maximum "amount specified for the gravest infringement".

2.13 The inference is therefore not that the appropriate penalty is calculated for each infringement and added together until the total penalty reaches the statutory maximum, but that the appropriate penalty is calculated for each infringement and that the largest penalty for any one infringement then reflects the absolute maximum can be imposed. This would be consistent with the sentencing principle of "totality"[9] where it is obligatory for the penalty setting tribunal to consider whether the total penalty is just and proportionate to the offending behaviour.

Do you have any other comments on the section on 'Statutory Background'?

2.14 The reference to action taken to mitigate the damage suffered by data subjects[10] sets out that "measures that are only implemented after the start of the Commissioner's investigation are less likely to be regarded as a mitigating factor." This makes sense for general unlawful processing but not necessarily in relation to an investigation following notification of a personal data breach. Elements of the circumstances of that breach may only become apparent following an incident, particularly where threat actors are using hitherto unknown attack methodologies to expose data subjects to harm. Where an organisation is under an obligation to notify the Commissioner of a personal data breach under Article 33 of the GDPR, it must do so very quickly after having become aware of the personal data breach. All remedial measures taken post-breach will therefore be after the Commissioner's investigation has started.

2.15 It therefore would make sense for the Guidance to distinguish between own-volition investigations and investigations following Article 83 notification, to avoid unforeseen consequences in this respect.

3 Circumstances in which the Commissioner would consider it appropriate to issue a penalty notice.

Do you have any comments on our approach to assessing the seriousness of an infringement?

3.1 The Commissioner marks intentional or negligent infringements to be particularly serious. This may be justifiable, but it is noted that the Guidance sets out[11] that an intentional infringement includes circumstances in which: (a) senior management authorised the unlawful processing; or (b) a controller or processor conducted the processing despite advice about the risks involved with or with disregard for its existing internal policies.

3.2 The wording of the first example – namely where "senior management authorised the unlawful processing" – is ambiguously drafted. It is presumed that the intention is for the Commissioner to consider intentional infringements to include circumstances in which senior management were aware that processing would be unlawful and authorised it anyway. The wording as currently drafted suggests that the Commissioner will conclude that any circumstance in which senior management authorised processing that was unlawful will constitute negligent

[7] The statutory maximum being as set out in Article 83(3) of the UK GDPR

[8] Paragraph 31 of the Guidance

[9] Offences-Taken-into-Consideration-and-Totality-definitive-guideline-Web.pdf (sentencingcouncil.org.uk)

[10] Paragraph 74 to 77

[11] Paragraph 65

processing, irrespective of the awareness of the lawfulness of processing by senior management.

3.3 Supplementary to 'the context and characteristics of the processing', the Commissioner should consider explicitly calling out 'the manner in which information was obtained' as a standalone factor for consideration in its assessment of the seriousness of the infringement. This is intended to highlight and dissuade evasive and non-transparent practices by controllers (e.g., engaging in indirect data collection and failing to meet transparency requirements.

3.4 Paragraph 59 includes the Commissioner considering less/non-tangible harms that individuals may suffer (e.g., distress and anxiety or loss of control) in its assessment of seriousness. It states as follows:

> *'The Commissioner's assessment of the level of damage suffered by data subjects will be limited to what is necessary to evaluate the seriousness of the infringement. Typically, it would not involve quantifying the harm, either in aggregate or suffered by specific people. It is also without prejudice to any decisions a UK court may make about awarding compensation for damage suffered.'*

3.5 It is our view that the Commissioner should go further than 'acting without prejudice with respect to decisions made by a UK court'. The Commissioner should actively review and keep in consideration the evolving position of the UK courts in their decisions relating to the award of compensation for non-tangible harm suffered. Whilst it may not be essential to quantify the harm as part of its assessment of seriousness, not taking into account harm would in our view be very unusual for a penalty setting regime. The Commissioner should consider applying thresholds to such non-tangible harms suffered to add some qualification to the severity of such harm alleged, i.e. the *de minimis* principle.[12] Taking an example, where distress is claimed by an impacted data subject as part of a complaint to the Commissioner and the Commissioner then opens an investigation and considers issuing a penalty notice, the Commissioner in its assessment should qualify the seriousness with reference to a qualifying criteria, such as the *de minimis* principle[13] when determining the 'level of damage suffered' (one of the considered factors).

3.6 The Guidance also suggests[14] that an infringement due to human error could indicate negligence on behalf of the organisation. The intention may be that human error that could have been avoided but for the negligence of the organisation – in not providing training to the individual that could have avoided the infringement, for example – but that is not clear. The inference is that the Commissioner could equate an honest mistake with negligence, of itself. This should be clarified.

Do you have any comments on our approach to assessing relevant aggravating and mitigating factors?

3.7 The guidance sets out that previous infringements will be considered an aggravating factor. However, the guidance does not reflect a similar mitigating factor for when there has been a previous history of compliance.

3.8 The Commissioner reflecting recognition for an otherwise unblemished record would be welcomed and would support the Commissioner's policy approach to accountability and to the Accountability Framework. An organisation that can furnish the Commissioner with documentary evidence demonstrating a history of compliance with the Commissioner's policy across the range of data protection management should rightly have that recognised by way of mitigation.

---

[12] Paragraph 15, TLT v Secretary of State for the Home Department, [2016] EWHC 2217 (QB).

[13] As referred to in the lineage of data protection compensation claims before the appellate courts, including, most recently, in *Rolfe & Ors -v- Veale Wasbrough Vizards LLP [2021] EWHC 2809 (QB)*

[14] Paragraph 67

3.9 With this in mind, we welcome the Commissioner's focus on the *effect* of any mitigating actions taken, rather than allowing arbitrary steps taken by organisations that appear to mitigate but have no operational application, such as the creation of paper-based policies. It may be useful for the Commissioner to provide further clarity to organisations that mere investment in 'data protection remediation' will not be sufficient to mitigate risk through the creation of boilerplate-style policies.

Do you have any comments on our approach to assessing whether imposing a fine is effective, proportionate and dissuasive?

3.10 The Guidance sets out[15] that when the Commissioner is considering whether it is "effective, proportionate and dissuasive" to issue a penalty, the primary consideration is whether it would be effective and dissuasive. The Guidance sets out that proportionality is a secondary analysis and only considered after it has been confirmed that the penalty would be effective and dissuasive.

3.11 It is therefore suggested that the Commissioner would not issue a penalty when it would be entirely justified to do so and proportionate to do so, but there is some reason it could not be effective or dissuasive to do so.

3.12 Article 83(1) of the UK GDPR sets out that a penalty *should* be effective, proportionate, and dissuasive and not that it *must* be. The use of the word "must" would reflect a requirement or obligation, as compared to the less absolute "shall," which suggests discretion in interpreting a preference for the thing to occur.

3.13 The Guidance confers a greater level of importance than the UK GDPR of the need for a penalty to be effective, proportionate, and dissuasive. The two-step process suggested by the guidance – consideration of whether it would be effective and dissuasive to impose a penalty before considering whether it would be proportionate – is also a non-statutory process that goes beyond the GDPR and could lead to unintended consequences.

4 Calculation of the appropriate amount of the fine

Do you have any comments on calculating the starting point for the fine based on the seriousness of the infringement?

4.1 The Guidance includes[16] that the Commissioner will use a starting point of between 0% and 10% of the relevant legal maximum, for infringements at the lower degree of seriousness.

4.2 The inference is therefore that the Commissioner would or could undertake the process set out in the guidance and conclude as following:

a. the seriousness of the infringement and aggravating and mitigating factors justify the imposition of a financial penalty, which would be an effective, proportionate, and dissuasive outcome; and

b. nevertheless conclude that the seriousness of the infringement, taken in isolation, could justify a starting point for the penalty at 0% of the legal maximum.

4.3 It is not clear how this could operate in practice and reference to a range of "up to 10%" would be a little clearer than the current reference suggesting a penalty range of "0% to 10%".

4.4 Whilst we note the Commissioner states that there is no 'pre-set 'tariff' of starting points for different types of infringement', the guidance would also benefit from setting out that historic

[15] Paragraph 104

[16] Paragraph 110

fines issued by the Commissioner would be considered, in the form of an alignment/benchmarking exercise. This is worth explicitly setting out in the guidance for clarity.

Do you have any comments on our approach to accounting for turnover when calculating the fine?

4.5 The guidance would benefit from further clarity regarding international undertakings, where for example a group parent company is based outside of the UK and the steps the Commissioner would take in such an instance to ascertain the worldwide turnover of the group of undertakings, where it may not be readily available (i.e. not a publicly listed entity).

Do you have any comments on how we apply aggravating and mitigating factors when calculating the fine?

4.6 Given step 4 of the assessment of the fine is so context-specific, we recognise the need for discretion to be applied on a case-by-case basis. However, if further case studies and examples can be provided to contextualise the application of step 4, that would assist organisations to be able to better predict the implications of their actions.

Do you have any comments on how we make any necessary adjustments to ensure the fine is effective, proportionate, and dissuasive?

4.7 Taking note of the Competition and Markets Authority's (CMA) method of calculation for fines issued, there is a specific step dedicated to settlement discounts. We suggest the Commissioner adopts a similar stance to the CMA and permits organisations to engage in formal settlement discussions and permitting a discount for any settlement, where the infringing party admits its participation in the infringement. We suggest this is clearly set out in the guidance.

Do you have any other comments on our five-step approach to the calculation of the appropriate amount of a fine?

4.8 The guidance would benefit from some examples of infringement case studies and where the Commissioner perceives each infringement to sit with respect to the ICO's scale of seriousness. Additionally or alternatively, the examples provided at the end of paragraph 134 would benefit from additional practical context with respect to the seriousness of offences.

4.9 We note that the five-step methodology for penalty setting follows the factors set out in article 83 and mirrors the European Data Protection Board position, which we regard as helpful and keeps the UK in broad alignment with the regulation and with the position in the EU.

5 Financial hardship

Do you have any comments on our approach to financial hardship?

5.1 The approach to financial hardship relates to the exceptional circumstance in which the Commissioner reduces a fine where the organisation is unable to pay because of its financial position.

5.2 While that makes sense and is consistent with the spirit of promotion economic growth, the issue of whether an organisation can adequately pay a penalty to the Commissioner is already “baked in” to the guidance. The earlier analysis of whether it would be effective, persuasive, and dissuasive to impose a penalty would mean that both the Commissioner and the organisation under analysis would have an opportunity to carefully consider this issue.

5.3 The process either would have failed if a penalty were imposed that was disproportionate to the means of the organisation to pay it, or the circumstances of the financial hardship would have to have come into being since the analysis was undertaken. The Guidance should be clearer on this point, or it may allow for the Commissioner to impose a disproportionate penalty on the basis that the organisation can then plead for clemency after the event: which could lead to perverse outcomes.

5.4 Financial hardship can also be mitigated by allowing the organisation time to pay. Other regimes have adopted this approach and it introduces the additional benefit of payments being a timely reminder of the importance of continued compliance.

6 Any other comments

Do you have any other comments on the draft Data Protection Fining Guidance?

6.1 The Guidance states[17] that it will not only apply to new investigations but also with respect to existing cases for which the Commissioner has not yet issued a penalty or intent to impose a penalty.

6.2 While retrospective effect in this way is not unheard of, the general position is that public interest in law not having retrospective effect must be outweighed by any competing public interest. It is unclear how that is the case here, and whether that will require a subjective assessment on investigations as they proceed to penalty each time. The Guidance should make that clearer.

DLA PIPER UK LLP
4 DECEMBER 2023

[17] Paragraph 10