Information Commissioner's Office

Information Commissioner

Data Protection Fining Guidance

March 2024

Presented to Parliament pursuant to Section 160(11) of the Data Protection Act 2018

Information Commissioner

Data Protection Fining Guidance

March 2024

Presented to Parliament pursuant to Section 160(11) of the Data Protection Act 2018

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ISBN 978-1-5286-4719-9

E03080084 03/24

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

Contents

About this guidance

1. The Information Commissioner (the Commissioner) is responsible for monitoring and enforcing the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

2. This guidance sets out the circumstances in which the Commissioner would consider it appropriate to exercise administrative discretion to issue a penalty notice. The Commissioner can issue penalty notices for infringements of the UK GDPR, Part 3 DPA 2018 (Law Enforcement Processing) or Part 4 DPA 2018 (Intelligence Services Processing). The Commissioner can also issue penalty notices for a failure to comply with an information notice, an assessment notice or an enforcement notice given under Part 6 DPA 2018. This guidance also explains how the Commissioner determines the amount of any fine imposed.

3. The Commissioner has published this guidance in performance of the statutory obligation to publish guidance about penalty notices, as set out in section 160 DPA 2018. The Commissioner will have regard to this guidance when deciding whether to issue a penalty notice and when setting the amount of any fine. It has been presented to Parliament pursuant to Section 160(11) DPA 2018.

4. This guidance replaces the sections about penalty notices in the Regulatory Action Policy published in November 2018. That policy previously set out the Commissioner's guidance on when issuing a penalty notice is appropriate[1] and the approach to determining the amount of any fine.[2]

[1] Regulatory Action Policy, page 24.
[2] Regulatory Action Policy, page 27.

Statutory background

5. Section 155 DPA 2018 sets out the Commissioner's power to issue penalty notices.

6. As explained in more detail below, the Commissioner may impose a fine where a person has failed:

or is failing, to comply with certain provisions of the UK GDPR or DPA 2018[3]; or

to comply with an information notice, assessment notice or enforcement notice given under Part 6 DPA 2018.[4]

7. The Commissioner can only exercise the powers to impose fines under Article 58(2)(i) and Article 83 UK GDPR by giving a penalty notice in accordance with section 155 DPA 2018.[5]

8. Section 160(1)(d) DPA 2018 requires the Commissioner to produce and publish guidance about how the Commissioner proposes to exercise functions in connection with penalty notices. The Commissioner's guidance must explain:

   - the circumstances in which the Commissioner would consider it appropriate to issue a penalty notice; and
   - how the Commissioner will determine the amount of the fine.[6]

9. Before finalising this guidance, the Commissioner consulted the Secretary of State and conducted a public consultation.[7] The Commissioner has also arranged to lay the finalised guidance before Parliament.[8]

10. This fining guidance applies from the date of publication to new cases relating to infringements of the UK GDPR or DPA 2018. It also applies to ongoing cases in which the Commissioner has not yet issued a notice of intent to impose a fine.[9]

[3] Section 155(1)(a) DPA 2018.
[4] Section 155(1)(b) DPA 2018.
[5] As specified by s115(9) DPA 2018
[6] Section 160(7)(a) and (c) DPA 2018. Section 160(7) also requires the Commissioner to produce and publish statutory guidance about (i) the circumstances in which the Commissioner would consider it appropriate to allow a person to make oral representations about the Commissioner's intention to give the person a penalty notice (section 160(7)(b)) and (ii) how the Commissioner will determine how to proceed if a person does not comply with a penalty notice (section 160(7)(d)). This guidance is currently set out in the Regulatory Action Policy.
[7] As required by section 160(9) DPA 2018.
[8] As required by section 160(11) DPA 2018.
[9] Schedule 16, paragraph 2(1) DPA 2018.

The infringements of UK GDPR and DPA 2018 for which the Commissioner can impose a fine

11. The Commissioner may impose a fine when satisfied that a person has failed to comply with the provisions of the UK GDPR or DPA 2018 referred to in section 149(2) to (5) DPA 2018.

12. In summary, these are:

- Where a controller or processor has failed, or is failing, to comply with provisions of UK GDPR or DPA 2018 relating to:
  - the principles of processing;
  - rights conferred on data subjects;
  - obligations placed on controllers and processors, including the requirement to communicate a personal data breach to the Commissioner; or
  - the principles for transfers of personal data outside the UK.[10]

Where a monitoring body has failed, or is failing, to comply with an obligation about the monitoring of approved codes of conduct.[11]

Where a certification provider does not meet the requirements for accreditation or has failed, or is failing, to comply with obligations under UK GDPR about the certification of controllers and processors, or any other provision of the UK GDPR (whether in its capacity as a certification provider or otherwise).[12]

Where a controller has failed, or is failing, to comply with a requirement to pay charges to the Commissioner.[13]

The Commissioner can also impose a fine on a person for failure to comply with requirements imposed on them under section 142 DPA 2018 (information notices), section 146 DPA 2018 (assessment notices), and section 149 DPA 2018 (enforcement notices).[14]

13. This includes failing to:

- provide information that the Commissioner reasonably requires;
- allow the Commissioner to inspect or examine documents,

[10] Section 149(2) DPA 2018.
[11] Section 149(3) DPA 2018.
[12] Section 149(4) DPA 2018.
[13] Section 149(5) DPA 2018. The Commissioner may only impose fixed penalties for a failure to comply with a requirement to pay charges to the Commissioner (see section 158 DPA 2018). The Commissioner's guidance on fixed penalties is currently set out in the Regulatory Action Policy, page 28.
[14] Section 155(1)(b) DPA 2018.

information, equipment or material; or

- comply with a requirement set out in an enforcement notice, such as a requirement to rectify or erase personal data or otherwise comply with the UK GDPR or DPA 2018.

14. **Annex 1** provides a table setting out the provisions of UK GDPR and DPA 2018 in relation to which the Commissioner can impose a fine.

The factors the Commissioner will take into account when deciding whether to issue a penalty notice and in determining the amount

15. When deciding whether to issue a penalty notice, and in determining the amount of the fine, the Commissioner must have regard (so far as relevant) to the factors listed in Articles 83(1) and (2) UK GDPR (for processing that falls under the UK GDPR) or section 155(3) DPA 2018 (for processing that falls under Part 3 or Part 4 DPA 2018 or a failure to comply with an information notice, assessment notice or enforcement notice).[15] These factors include the requirement that, in each individual case, a fine imposed by the Commissioner must be effective, proportionate and dissuasive.[16]

16. The factors set out in Article 83(2) UK GDPR[17] that the Commissioner must have regard to are:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32 UK GDPR;

(e) any relevant previous infringements by the controller or processor;

[15] Section 155(2) DPA 2018.
[16] Article 83(1) UK GDPR and section 155(3)(l) DPA 2018. See further below for an explanation of how the Commissioner assesses whether a penalty is effective, proportionate and dissuasive.
[17] A similar list of factors is set out in section 155(3) DPA 2018 in relation to penalties imposed in respect of infringements of the DPA 2018.

(f) the degree of cooperation with the Commissioner, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the Commissioner, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) UK GDPR have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 UK GDPR or approved certification mechanisms pursuant to Article 42 UK GDPR; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

17. Please see Circumstances in which the Commissioner would consider it appropriate to issue a penalty notice for a detailed explanation as to how the Commissioner takes these factors into account.

The maximum amount of a fine under UK GDPR and DPA 2018

18. The amount of the fine that the Commissioner can impose for an infringement of UK GDPR or DPA 2018 is subject to a statutory maximum.[18]

19. Article 83 UK GDPR and section 157 DPA 2018 provide for two levels of maximum fine, depending on the statutory provision that has been infringed. These are referred to as the 'standard maximum amount' and the 'higher maximum amount'. The tables in **Annex 2** set out which level of maximum fine applies to the relevant provisions of the UK GDPR and DPA 2018, as set out in Article 83(4) and (5) UK GDPR and section 157(2), (3) and (4) DPA 2018.

20. The maximum fine amounts for each level differ based on whether the controller or processor is an 'undertaking'[19], as follows:

The **standard** maximum amount is £8.7 million or, in the case of an undertaking, is the higher of either £8.7 million or 2% of the undertaking's total

[18] Section 157 DPA 2018.

[19] See The concept of an 'undertaking' for the purpose of imposing fines for an explanation of the term 'undertaking' in this context.

worldwide annual turnover in the preceding financial year.20

The higher maximum amount is £17.5 million or, in the case of an undertaking, is the higher of either £17.5 million or 4% of the undertaking's total worldwide annual turnover in the preceding financial year.[21]

21. This means that the applicable statutory maximum amount is only calculated by reference to a percentage of turnover where an undertaking's total worldwide annual turnover exceeds:

    - £435 million in relation to the standard maximum amount (the 2% percentage figure applies); or

£437.5 million in relation to the higher maximum amount (the 4% percentage figure applies).[22]

The concept of an 'undertaking' for the purpose of imposing fines

22. Where a controller or processor forms part of an undertaking, for example where a controller is a subsidiary of a parent company, the Commissioner will calculate the maximum fine based on the turnover of the undertaking as a whole.[23]

23. The UK GDPR and DPA 2018 do not define the term 'undertaking' in the context of imposing fines.[24] However, the recitals to the UK GDPR are clear that an 'undertaking' for these purposes should be understood in accordance with UK competition law.

24. Recital 150 UK GDPR states that 'an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102' of the Treaty on the Functioning of the EU (TFEU). Articles 101 and 102 TFEU set out prohibitions on anti-competitive agreements between undertakings and anti-competitive conduct by dominant undertakings.[25] In applying the EU GDPR, the European Data Protection Board (EDPB) considers the case law of the Court of Justice of the EU in the field of competition law to be

[20] Article 83(4) UK GDPR and section 157(6) DPA 2018.
[21] Article 83(5) UK GDPR and section 157(5) DPA 2018.
[22] This is because 2% of turnover of £435 million is £8.7 million and 4% of turnover of £437.5 million is £17.5 million.
[23] Further detail about how the Commissioner will calculate the turnover of an undertaking is set out in Determination of total worldwide annual turnover below.
[24] Note that the concept of an 'undertaking' for the purpose of imposing a fine under UK GDPR and DPA 2018 should be distinguished from the use of the terms 'enterprise' and 'group of undertakings' defined in Article 4(18) and (19) UK GDPR, which primarily relate to provisions in Chapter V UK GDPR (Transfers of personal data to third countries or international organisations).
[25] The equivalent provisions in UK law are set out in the Competition Act 1998.

relevant when assessing the turnover to be taken into account in the context of verification of the upper limit of the fine amount.[26]

25. While Articles 101 and 102 TFEU and EDPB decisions no longer apply to the UK following the UK's exit from the European Union[27], the concept of an 'undertaking' is well established in UK competition law through UK and retained EU case law.

26. An 'undertaking' refers to any entity that is engaged in economic activity, regardless of its legal status or the way in which it is financed.[28] An entity is engaged in an 'economic activity' where it conducts any activity consisting in offering goods or services on a given market.[29] The fact that an entity is not motivated by profit or does not have an economic purpose does not, in itself, mean that it does not engage in economic activity.[30] Public authorities, state-controlled enterprises and charities may therefore all fall within the definition of an undertaking if they are carrying on an economic activity.[31]

27. In this context, an undertaking does not correspond to the commonly understood notion of a legal entity or a company under, for example, English commercial or tax law.[32] Instead, an undertaking may comprise one or more legal or natural persons forming a 'single economic unit', rather than a single entity characterised as having a legal personality.[33]

28. Whether or not an individual controller or processor forms part of a wider undertaking depends on whether it can act autonomously or whether another legal or natural person, for example a parent company, exercises decisive influence over it. In considering whether a parent company has decisive influence over a controller or processor (and therefore forms part of the same single economic unit), the Commissioner takes into account all relevant factors about the economic, organisational and legal links which tie

[26] See EDPB, Binding Decision 1/2021, WhatsApp Ireland, adopted on 28 July 2021, paragraph 289. The Court of Justice of the EU has confirmed this approach, see: *Deutsche Wohnen SE v Staatsanwaltschaft Berlin*, C-807/21, EU:C:2023:950, paragraph 59.

[27] Although EDPB decisions and guidance have no legal force in the UK, the Commissioner may have regard to them if the Commissioner considers it appropriate to do so. For example, where the decision or guidance is relevant to a similar matter being considered under UK data protection law.

[28] See, for example, the Competition Appeal Tribunal's judgment in *Sainsbury's Supermarkets v Mastercard Inc*. [2016] CAT 11 at paragraph 353, citing *Hofner and Elser v Macrotron GmbH*, C-41/90, EU:C:1991:161, paragraph 21.

[29] *Pavel Pavlov v Stichting Pensioenfonds Medische Specialisten*, C-180/98, EU:C:2000:428, paragraph 75.

[30] For example, see *Laurent Piau v European Commission*, T-193/02, EU:T :2005:22, paragraph 69, where the EU General Court held that football is an economic activity for football clubs and that they are therefore undertakings within the meaning of competition law.

[31] See Office of Fair Trading decision, Exchange of information on future fees by certain independent fee-paying schools, (Case CA98/05/2006), 20 November 2006, paragraphs 1312 to 1320.

[32] *Sepia Logistics Ltd (formerly known as Double Quick Supplyline Limited) v Office of Fair Trading* [2007] CAT 13, paragraph 70.

[33] *Sepia Logistics Ltd (formerly known as Double Quick Supplyline Limited) v Office of Fair Trading* [2007] CAT 13, paragraph 70; *Sainsbury's Supermarkets v Mastercard Inc.* [2016] CAT 11, paragraphs 356 and 357.

the relevant subsidiary to the parent company.[34] Such evidence will vary from case to case, but may, for example, include the level of shareholding a parent company has in its subsidiary and the representation it has on the subsidiary's board. It may also include other evidence of the influence the parent company has over a subsidiary's conduct and operations. This could include its influence over the way the subsidiary provides goods or services to data subjects or processes their personal data.

29. Where a parent company owns all, or nearly all, the voting shares in a subsidiary there is a presumption that the parent company exercises decisive influence over the subsidiary's conduct. This presumption may be rebutted. However, the burden is on the parent company to provide sufficient evidence to demonstrate that the subsidiary acts independently.[35]

30. As well as using the concept of the undertaking for determining the relevant maximum amount, the Commissioner may also hold a parent company jointly and severally liable for the payment of a fine imposed on a controller or processer over which the parent company has decisive influence.[36]

The Commissioner's approach to fines where there is more than one infringement by a controller or processor

31. In many cases, a controller or processor's conduct may infringe more than one provision of the UK GDPR or Part 3 or Part 4 DPA 2018.

32. This situation is addressed by Article 83(3) UK GDPR, which states that 'if a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of the [UK GDPR], the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement'.[37] In other words, where the Commissioner finds that the 'same or linked processing operations' infringe more than one provision of UK GDPR, the overall fine imposed by the Commissioner in relation to the infringements arising from those processing

[34] See, for example, *Akzo Nobel v European Commission*, C-97/08P, EU:C:2009:536, paragraph 58 and *Durkan v Office of Fair Trading*, [2011] CAT 6, paragraph 22.
[35] *Akzo Nobel v European Commission*, C-97/08P, EU:C:2009:536, paragraphs 60 and 61. See also *Goldman Sachs v European Commission*, C-595/18P, EU:C:2021:73, paragraphs 31 to 36.
[36] See the Commissioner's decision of 4 April 2023 in TikTok Information Technologies UK Limited and TikTok Inc, paragraph 190 and EDPB, Binding Decision 1/2021, WhatsApp Ireland, adopted on 28 July 2021, paragraph 290. See also, by analogy, the position under competition law as set out in, for example, *Durkan v Office of Fair Trading* [2011] CAT 6, paragraph 15 and *Sainsbury's Supermarkets v Mastercard Inc.* [2016] CAT 11, paragraphs 363(22).
[37] Article 83(3) UK GDPR. The DPA 2018 does not include an equivalent provision to Article 83(3) UK GDPR in respect of processing under the DPA 2018. However, to ensure consistency the Commissioner will take the same approach in determining penalties in respect of infringements of DPA 2018 as the Commissioner would in respect of infringements of the UK GDPR.

operations must not exceed the maximum statutory amount that applies to the most serious of the individual infringements identified.[38]

33. To determine whether Article 83(3) applies to limit the total amount of the fine that can be imposed, the Commissioner will consider in each case whether:

- the controller or processor's conduct gives rise to more than one infringement resulting from the 'same or linked processing operations'; or
- the controller or processor has engaged in separate forms of conduct involving different processing operations that are not the 'same or linked' and have given rise to separate infringements.

34. The Commissioner's approach is explained in more detail below.

More than one infringement arising from the 'same or linked' conduct

35. The Commissioner will assess on a case-by-case basis whether more than one infringement relates to the same or linked processing operations.

36. As defined in section 3(4) DPA 2018 and Article 4(2) UK GDPR, 'processing' means an 'operation or set of operations' that is performed on personal data or sets of personal data. The definitions in the DPA 2018 and UK GDPR each set out a non-exhaustive list of such processing operations.

37. To lawfully carry out a processing operation or set of processing operations, the controller or processor must comply with a range of provisions in the UK GDPR or Part 3 or Part 4 DPA 2018. For example, a controller must have a lawful basis for processing the information. It must also comply with the relevant transparency obligations. Accordingly, the same processing operation or set of processing operations may lead to more than one infringement of UK GDPR or Part 3 or Part 4 DPA 2018.[39]

38. Similarly, different processing operations or sets of processing operations may be sufficiently 'linked' such that they form part of the same overall conduct. This may, in turn, lead to the controller or processor infringing more than one provision of the UK GDPR or Part 3 or Part 4 DPA 2018.

39. In determining whether processing operations are linked and form part of the same overall conduct, the Commissioner will have regard to the relevant circumstances of the case. In particular, this will include assessing the extent to which the infringements arise from conduct that involves a series of closely-related processing operations. Relevant factors are likely to

[38] See EDPB, Binding Decision 1/2021, WhatsApp Ireland, adopted on 28 July 2021, paragraphs 315 to 327.
[39] For example, see the Commissioner's decision of 4 April 2023 in TikTok Information Technologies UK Limited and TikTok Inc, which found infringements of Article 5(1)(a), Article 8, Article 12 and Article 13 UK GDPR.

include the extent to which the processing operations or set of processing operations are:

- aimed at achieving a particular purpose or form part of the same means of processing determined by a controller;
- related to the same, or a similar group of, data subjects; and
- carried out concurrently, sequentially or otherwise in a way that is proximate in time.

40. Where the Commissioner finds that a controller or processor's overall conduct has infringed more than one provision of the UK GDPR, the Commissioner will apply Article 83(3) UK GDPR and identify the statutory maximum applicable to the most serious individual infringement. To ensure consistency, the Commissioner will take the same approach when assessing whether there has been infringement of Part 3 or Part 4 DPA 2018.

41. In such cases, the Commissioner may decide to impose a fine for each infringement arising from the same or linked processing operations, provided that the sum of those penalties does not exceed the applicable statutory maximum.[40] For example, the Commissioner may decide to impose a fine on an information society service for an infringement of Article 8 UK GDPR and a fine for an infringement of Article 13 UK GDPR that relate to the same or linked processing operations. The total fine must not exceed the statutory maximum for the gravest infringement under Article 83(4) and (5) UK GDPR. In this example, that is the Article 13 UK GDPR infringement (which is subject to the higher maximum amount of £17.5 million or 4% of turnover).[41] Therefore, if the Commissioner imposes a fine for the infringement of Article 8 and a fine for the infringement of Article 13, the combined total of the two fines must not exceed £17.5 million or 4% of turnover (whichever is higher).

Separate infringements arising from separate conduct

42. By contrast, an investigation may identify that different forms of conduct by a controller or processor have infringed separate provisions of the UK GDPR or Part 3 or Part 4 DPA 2018 (ie circumstances where the processing operations are not sufficiently linked).

43. For example, during an investigation about a controller's security breach involving the disclosure of its employees' salaries and bank account details, the Commissioner may also obtain evidence that the controller had not

[40] See EDPB, Binding Decision 1/2021, WhatsApp Ireland, adopted on 28 July 2021, paragraphs 315 to 327.
[41] Article 83(5)(b) provides that an infringement of data subjects' rights pursuant to Articles 12 to 22 are subject to the highest maximum amount. Article 83(4)(a) provides that the obligations of the controller and the processor pursuant to Article 8, among others, are subject to the standard maximum amount.

complied with its transparency obligations in respect of its direct marketing activities.

44. In such a case, the Commissioner may decide to include the separate infringements in the same penalty notice, particularly if it would streamline the procedure and avoid duplication of effort (on the part of both the party involved and the Commissioner).[42] However, Article 83(3) UK GDPR would not apply because the infringements involve separate conduct and do not relate to the same or linked processing operations (in this example, one infringement relates to processing that led to a security breach; the other infringement relates to processing involving a failure under the transparency obligations). Therefore, the fine imposed for each infringement would be subject to the relevant statutory maximum amount applicable to each infringement (as specified in Article 83(4) and (5) UK GDPR).

Restrictions on issuing penalty notices

45. Under the DPA 2018, in certain circumstances the Commissioner is restricted from issuing penalty notices or subject to additional requirements. These circumstances are:

    - **Processing data for the 'special purposes'**: The Commissioner may only issue a penalty notice to a controller or processor with respect to the processing of personal data for the special purposes[43] in specific circumstances (as set out in section 156 DPA 2018).[44] These are that a determination under section 174 DPA 2018 has taken effect and a court has granted leave for the penalty notice to be given.

Houses of Parliament: The Commissioner may not issue a penalty notice with respect to the processing of personal data where the purposes and manner of the processing are determined by or on behalf of either the House of Commons or the House of Lords.[45]

The Crown Estate Commissioners and the Royal Household: The Commissioner may not issue a penalty notice to the Crown Estate Commissioners, or a person who is a controller acting on behalf of the Royal Household, the Duchy of Lancaster or the Duchy of Cornwall (as specified by section 209(4) DPA 2018).[46]

[42] In this example, the separate infringements would be (i) failure to comply with Article 5(1)(f) and Article 32 UK GDPR (in relation to the security breach) and (ii) failure to comply with Article 12 and Article 13 UK GDPR (in relation to transparency obligations). The alternative would be for the Commissioner to issue separate penalty notices, ie one for each of the separate infringements.
[43] The 'special purposes' are defined in section 174(1) DPA 2018 and mean one or more of the purposes of journalism, academic purposes, artistic purposes, or literary purposes.
[44] Section 156(1) and (2) DPA 2018.
[45] Section 156(3) DPA 2018.
[46] Section 156(4) DPA 2018.

Joint controllers – law enforcement or intelligence services processing: Where joint controllers process personal data to which Part 3 or Part 4 DPA 2018 applies (law enforcement processing or processing by the intelligence services), the Commissioner may only give the controller a penalty notice if the controller is responsible for compliance with the provision, requirement or principle in question.[47]

[47] Section 156(5) DPA 2018.

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

46. In deciding whether to issue a penalty notice to a person, the Commissioner will have regard (so far as relevant) to the matters set out in Article 83(1) and Article 83(2) UK GDPR or in s.155(3) DPA 2018. These factors are listed in The factors the Commissioner will take into account when deciding whether to issue a penalty notice and in determining the amount above.

47. The Commissioner can impose fines for a wide range of different infringements under the UK GDPR and DPA 2018. The Commissioner will assess each case individually, taking into account the relevant circumstances, before deciding whether it is appropriate to exercise the Commissioner's administrative discretion to issue a penalty notice.

48. Before taking a decision, the Commissioner will consider whether to impose a fine as well as, or instead of, other corrective measures.[48] For example, the Commissioner may decide to require a person to take certain steps specified in an enforcement notice to remedy an infringement, as well as imposing a fine.

49. The assessment of whether it is appropriate to issue a penalty notice in relation to a particular infringement is fact-specific and will depend on the circumstances of each individual case. The Commissioner is not bound by previous decisions, but will ensure there is broad consistency in the approach taken when assessing whether issuing a penalty notice is appropriate.

50. In carrying out the assessment of whether it is appropriate to issue a penalty notice the Commissioner will have regard to:

the seriousness of the infringement or infringements;

[48] Article 58(2) UK GDPR sets out the Commissioner's corrective powers under UK GDPR. In summary, these are: (a) to issue warnings; (b) to issue reprimands; (c) to order compliance with a data subject's requests to exercise their rights; (d) to order compliance with UK GDPR; (e) to order a personal data breach to be communicated to a data subject; (f) to impose a ban on processing; (g) to order the rectification or erasure of personal data; (h) to withdraw a certification, order a certification body to withdraw a certification, or order a certification body not to issue a certification; (i) to impose an administrative fine; and (j) to order the suspension of data flows to a recipient in a third country or an international organisation. As set out in section 115 DPA 2018, certain of these corrective powers can only be exercised by the Commissioner giving an enforcement notice under section 149 DPA 2018. The Commissioner has similar corrective measures available in respect of processing under Part 3 or Part 4 DPA 2018 (Section 149(2) DPA 2018 and Schedule 13, paragraph 2 DPA 2018).

any relevant aggravating or mitigating factors; and

whether imposing a fine would be effective, proportionate and dissuasive.

51. This section of the guidance sets out how the Commissioner will approach each of these considerations when deciding whether to issue a penalty notice.

52. If the Commissioner decides that it is appropriate to issue a penalty notice, the Commissioner will apply the methodology for determining the fine amount, as set out in Calculation of the appropriate amount of the fine below.

Seriousness of the infringement

53. The Commissioner will assess the seriousness of the infringement, taking into account:

its nature, gravity and duration[49];

whether it was intentional or negligent[50]; and

the categories of personal data affected.[51]

54. If the Commissioner decides that the infringement was serious, having regard to those factors, then it is likely that the Commissioner will issue a penalty notice, unless there are mitigating factors that outweigh that assessment (see Relevant aggravating or mitigating factors below).[52] However, where the assessment of seriousness is more finely balanced, the Commissioner may nevertheless issue a penalty notice where there are relevant aggravating factors. In either case, the Commissioner will also consider whether issuing a penalty notice is effective, proportionate and dissuasive.

55. The Commissioner's findings about the seriousness of the infringement will inform the starting point for the level of fine imposed (see Calculation of the appropriate amount of the fine below).

Nature, gravity and duration of the infringement

56. The assessment of the **nature** of the infringement involves consideration of the relevant circumstances of the case and the specific provision of the UK

[49] Article 83(2)(a) UK GDPR or section 155(3)(a) DPA 2018.
[50] Article 83(2)(b) UK GDPR or section 155(3)(b) DPA 2018.
[51] Article 83(2)(g) UK GDPR or section 155(3)(g) DPA 2018.
[52] As explained in Relevant aggravating or mitigating factors, mitigating factors may include, for example, any action taken by the controller or processor to mitigate the damage suffered by data subjects (Article 83(2)(c) UK GDPR or section 155(3)(c) DPA 2018), the degree of cooperation with the Commissioner (Article 83(2)(f) UK GDPR or section 155(3)(f) DPA 2018), or any other mitigating factor applicable to the circumstances of the case (Article 83(2)(k) UK GDPR or section 155(3)(k) DPA 2018).

GDPR or DPA 2018 that has been infringed. This includes taking into account whether:

the infringement prevented the provision concerned from being applied effectively or prevented the objective it sought to protect being fulfilled; and

the infringement is subject to the standard maximum fine or the higher maximum fine.

57. The assessment of the **gravity** of the infringement involves consideration of the:

nature of the processing;

scope of the processing;

purpose of the processing;

number of data subjects affected by the processing; and

level of damage suffered by data subjects affected by the processing.

58. In carrying out this assessment, the factors the Commissioner takes into account will include the following:

Nature of the processing: The Commissioner will consider the context and characteristics of the processing by the controller or processor, having regard to whether it involves business activities, charitable or other non-profit motives, or is carried out by a public body. The Commissioner may, depending on the context, give more weight to this factor if the nature of the processing is likely to result in high risk to data subjects, taking into account the Commissioner's published guidance. For example, 'high risk' processing may include processing operations that involve:

- the application of new or innovative technology;
- automated decision-making;
- the use of biometric or genetic data;
- monitoring or tracking; or
- invisible processing.

The Commissioner may also give more weight to this factor where:

- there is a clear imbalance of power between the data subjects and

the controller[53];

- the processing involves children's personal data[54]; or
- the processing involves personal data of other vulnerable people who need extra support to protect themselves.[55]

Scope of the processing: The Commissioner will consider the scope of the processing in terms of both its territorial scope (local, national or involving the international transfer of data) and the extent and scale of the processing. The Commissioner may give greater weight to this factor where the scope or scale of the processing is large and, for example, it involves systematic and extensive profiling of data subjects.

Purpose of the processing: The Commissioner will take into account the purpose of the processing carried out by the controller or processor. The Commissioner may give greater weight to this factor if the relevant processing is central to a controller or processor's main business and commercial activities, thereby forming a core part of its activities. This may, for example, be the case where a controller's business model and revenue relies on the processing of personal data for the purpose of direct marketing or targeted advertising. However, the Commissioner will also have regard to the purpose of the processing where it is not directly related to the controller or processor's core activities. This applies particularly where the processing may significantly affect people's rights and freedoms.

Number of data subjects affected: The greater the number of data subjects affected by the infringement, the more weight the Commissioner will give to this factor. In making the assessment, the Commissioner will take into account the number of data subjects potentially affected, as well as those actually affected, by the infringement. The Commissioner may also have regard to the number of complaints received from data subjects about the conduct that has led to the finding of the infringement or infringements. However, the absence of such complaints will not be regarded as an indication that conduct found to infringe UK GDPR or DPA 2018 is less serious.

Level of damage suffered: The Commissioner will consider the extent to which the infringement affected people's rights and freedoms or otherwise led to them suffering, or being likely to suffer, harm. The damage suffered may be physical,

[53] For example, Recital 43 to the UK GDPR explains that consent should not provide a valid legal ground for processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller. This includes where the imbalance arises from the market position of the controller.
[54] As set out in Recital 38 to the UK GDPR, children merit special protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.
[55] As set out in Recital 75 to the UK GDPR, risks may result where the personal data of vulnerable people, particularly children, are processed.

material or non-material.[56] Such damage may include actual or potential harm to data subjects in the form of, for example:

- physical or bodily harm;
- psychological harm;
- economic or financial harm;
- discrimination;
- reputational harm; or
- loss of human dignity.[57]

In carrying out the assessment of the level of damage, the Commissioner will take into account the fact that:

- some harms are more readily identifiable (for example, financial loss or identity theft) whereas others are less tangible (for example, distress and anxiety or loss of control over personal data); and
- where an infringement affects a large number of data subjects, it may result in a high degree of damage in aggregate and give rise to wider harm to society, even if the impact on each person affected is more limited.

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.[58]

The assessment of the **duration** of the infringement involves considering how long the infringement went on for. The longer the duration of the infringement, the more weight the Commissioner is likely to attribute to this factor. This is because of the greater potential for harm to have occurred. However, infringements of a short duration are not necessarily less serious. They may also lead to significant harm to data subjects.

In assessing seriousness in relation to failures to comply with information notices or assessment notices, the Commissioner will, in particular, take into account the extent to which the failure to comply is likely to negatively affect the

[56] Recital 75 UK GDPR.
[57] See ICO, Overview of Data Protection Harms and the ICO's Taxonomy, April 2022. In the context of this Fining Guidance, the ICO uses the terms 'damage' and 'harm' interchangeably.
[58] Any person who suffers damage as a result of an infringement has a right to receive compensation from the relevant controller or processor (see Article 82 UK GDPR and section 169 DPA 2018).

Commissioner's ability to act. This might be, for example, because the information is needed to progress an investigation or for the purpose of discharging another of the Commissioner's functions.

59. In assessing seriousness in relation to failures to comply with enforcement notices, the Commissioner will, in particular, take into account the extent to which the failure to comply has:

    - led, or is likely to lead, to further damage or distress to data subjects; or
    - resulted in the controller or processor obtaining an advantage or deriving a benefit from the failure.

Intentional or negligent character of the infringement

60. The Commissioner will consider whether the infringement was intentional or negligent as part of the assessment of its seriousness.[59] Where there is evidence of intent on the part of the controller or processor, the Commissioner may regard the infringement as particularly serious and may therefore be more likely to issue a penalty notice. Negligent infringements can also be serious. The Commissioner may also decide to issue a penalty notice in case where the controller or processor is found to be negligent.

61. In this context, an infringement is committed intentionally where the evidence shows the controller or processor knew its conduct was likely to constitute an infringement of the UK GDPR or DPA 2018, but it either deliberately continued with the conduct or was indifferent to whether it infringed UK GDPR or DPA 2018. In other words, the controller or processor wilfully ignored the known risk of its conduct infringing the law.

62. The circumstances that the Commissioner considers may indicate an intentional infringement include where:

    - senior management authorised the unlawful processing; or
    - a controller or processor carried out the processing despite advice about the risks involved (including where the risks had been brought to its attention by an individual, the Commissioner or other third party) or with disregard for its existing internal policies.

63. An infringement is committed negligently where the controller or processor breached the duty of care required by UK GDPR or DPA 2018. Therefore, the Commissioner may issue a penalty notice for an infringement of UK

[59] Article 83(2)(b) UK GDPR and section 155(3)(b) DPA 2018. See also *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (NVSC) v Valstybinė duomenų apsaugos inspekcija (Lithuanian Data Protection Inspectorate)*, Case C-683/21, EU:C:2023:949, paragraph 86.

GDPR or DPA 2018 where the controller or processor's failure to comply with its statutory obligations was unintentional.[60]

64. In assessing negligence, the Commissioner will take into account all relevant evidence about whether the controller or processor breached the duty of care required by law. This requires taking into account the individual circumstances of each case in order to establish the controller or processor's liability. However, the Commissioner's assessment is likely to include, for example, considering evidence about the extent to which the infringement resulted from the controller or processor:

failing to adopt policies aimed at ensuring compliance with data protection law;

failing to read and abide by its existing data protection policies or, where relevant, failing to take steps to comply with a code of conduct of which it is a member or meet the criteria of a certification mechanism;

infringing UK GDPR or DPA 2018 through human error, particularly where the person (or people) involved had not received adequate training on data protection risks;

failing to check for personal data in information that is published or otherwise disclosed; or

failing to apply technical updates in a timely manner.

65. In relation to a failure to comply with an information notice or assessment notice, the Commissioner will also consider whether the controller, processor or (in the case of an information notice) any other person has a reasonable excuse for failing to comply. The circumstances that may constitute a reasonable excuse are not fixed. The Commissioner will assess on a case-by-case basis whether any reasons for a failure to comply amount to a reasonable excuse. The Commissioner will take into account how far a significant and genuinely unforeseeable or unusual event beyond the person's control caused the failure. However, the Commissioner is unlikely to consider that a person has a reasonable excuse in circumstances where they have not, in the Commissioner's view, otherwise made reasonable efforts to comply with the notice.

[60] See Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253, adopted on 3 October 2017. See also, in relation to the application of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) [2016] OJ L 119/1, the Court of Justice of the EU's findings in *NVSC v Lithuanian Data Protection Inspectorate*, paragraph 81 ('a controller may be penalised for conduct falling within the scope of the GDPR where that controller could not have been unaware of the infringing nature of its conduct, whether or not it was aware that it was infringing the provisions of the GDPR') and paragraph 82 ('it is not necessary for there to have been action by, or even knowledge on the part of, the management body' for Article 83 GDPR to apply).

66. In carrying out the assessment, the Commissioner will also take into account the fact that controllers are responsible for compliance with the data protection principles and for implementing appropriate technical and organisational measures to demonstrate compliance with UK GDPR or Part 3 or Part 4 DPA 2018.[61] Where there are two or more joint controllers, the Commissioner will assess the responsibility of each of the controllers for the infringement to determine whether any or all of them acted intentionally or negligently. Processors also have a range of obligations under UK GDPR and Part 3 and Part 4 DPA 2018, particularly in relation to the security of personal data.[62] The Commissioner therefore also expects processors to take responsibility, where applicable, for evaluating risks and implementing measures to mitigate them.[63]

Categories of personal data affected by the infringement

67. The categories of personal data affected by the infringement are also relevant to the assessment of seriousness. The UK GDPR and Part 3 and Part 4 DPA 2018 make clear that the processing of certain categories of personal data deserves special protection. These categories include:

special category data (Article 9 UK GDPR);

personal data relating to criminal convictions and offences (Article 10 UK GDPR); and

personal data falling within the definitions of 'sensitive processing' in Part 3 and Part 4 DPA 2018.[64]

68. The Commissioner is likely to consider infringements involving the processing of such data as being particularly serious.

69. In assessing seriousness, the Commissioner may also take into account other types of personal data affected by the infringement where that data may be regarded as particularly sensitive. This includes where the dissemination of the personal data is likely to cause damage or distress to data subjects, for example:

- location data;
- private communications (particular those involving intimate details or confidential information about the data subject);

[61] See Article 5(2) and Article 24 UK GDPR and sections 56 and 102 DPA 2018.
[62] See Article 32 UK GDPR and sections 66 and 107 DPA 2018.
[63] See Recital 83 UK GDPR. Note also that the responsibility and liability of a controller for the conduct of a processor does not extend to situations where the processor has processed personal data for its own purposes or the processor has processed personal data in a way that is incompatible with the arrangements determined by the controller such that the controller cannot reasonably be considered to have consented to the processing (see *NVSC v Lithuanian Data Protection Inspectorate*, paragraph 85).
[64] See section 35(8) DPA 2018 and section 86(7) DPA 2018.

- passport or driving licence details; or
- financial data.

Relevant aggravating or mitigating factors

70. Having assessed the seriousness of the infringement, the Commissioner will take into account any relevant aggravating or mitigating factors. These factors will inform the Commissioner's decision about whether it is appropriate to issue a penalty notice in the individual circumstances of the case.

Action taken to mitigate the damage suffered by data subjects

71. The Commissioner will have regard to any action taken by the controller or processor to mitigate the damage suffered by data subjects.[65]

72. When an infringement of the UK GDPR takes place, a controller or processor should take steps to mitigate the harmful consequences of the infringement for the data subjects concerned. The Commissioner may consider any actions taken by the controller or processor to mitigate the damage suffered as a mitigating factor.

73. The Commissioner will consider when the controller or processor took any such action and, if so, whether the measures implemented were appropriate and effective in mitigating the damage suffered by data subjects. If the action taken had no effect (or only a limited effect) on mitigating the damage suffered by the data subjects, the Commissioner is likely to give it less weight.

74. The Commissioner is more likely to take into account measures implemented prior to the controller or processor becoming aware of the Commissioner's investigation as a mitigating factor. Measures that are only implemented after the start of the Commissioner's investigation are less likely to be regarded as a mitigating factor. Where a controller is under a statutory duty to notify the Commissioner of a personal data breach it can still benefit from this mitigating factor. Therefore, this mitigating factor may apply even if the controller takes steps to implement such measures after informing the Commissioner about the personal data breach.[66] However, in order for the mitigating factor to apply, the Commissioner expects the controller to take steps to mitigate any damage in a timely manner.

The degree of responsibility of the controller or processor

75. The Commissioner will have regard to the degree of responsibility of the controller or processor, taking into account technical and organisational

[65] Article 83(2)(c) UK GDPR. Section 155(3)(c) DPA 2018 is similarly worded: 'any action taken by the controller or processor to mitigate the damage or distress suffered by the data subjects'.
[66] See Article 33 UK GDPR, section 67 DPA 2018, and section 108 DPA 2018.

measures implemented by them pursuant to Articles 25 and 32 UK GDPR or in accordance with sections 57, 66, 103 and 107 DPA 2018.[67]

76. Controllers and processors are required and expected to take responsibility for complying with their obligations under the UK GDPR or Part 3 or Part 4 DPA 2018. In assessing this factor, the Commissioner will consider how far the controller or processor did what it could be expected to do in terms of implementing technical and organisational measures, taking into account:

- its size and resources; and
- the nature and purpose of the processing.

77. Where relevant, the Commissioner will also take into account any shared responsibility between controllers or between controllers and processors.

78. In the light of the level of accountability expected of controllers and processors under UK GDPR and Part 3 and Part 4 DPA 2018, it is more likely that the Commissioner will consider the degree of responsibility to be an aggravating factor or, at best, a neutral factor. In order for this to be considered a mitigating factor, a controller or processor will need to show that it has gone over and above its obligations under UK GDPR and DPA 2018.

Relevant previous infringements by the controller or processor

79. The Commissioner will have regard to the extent to which any previous infringements by a controller or processor may be considered an aggravating factor.[68]

80. Previous infringements that concern a similar subject matter, or infringements that occurred recently, are more likely to be relevant. The Commissioner will therefore give these greater weight.

81. However, the Commissioner may also give weight to previous infringements relating to a different subject matter if they arose in a similar manner. Further, if a controller or processor has repeatedly infringed the UK GDPR or DPA 2018, the Commissioner is likely to take this into account as an aggravating factor if it demonstrates a generally lax attitude towards compliance.

82. The Commissioner will not consider the absence of any previous infringements to be a mitigating factor because compliance with the UK GDPR and DPA 2018 is expected.

[67] Article 83(2)(d) UK GDPR and section 155(3)(d) DPA 2018.
[68] Article 83(2)(e) UK GDPR. Section 155(3)(e) DPA 2018 refers to 'any relevant previous failures by the controller or processor'.

The degree of cooperation with the Commissioner

83. The Commissioner will have regard to the degree of cooperation with the Commissioner, in order to remedy the infringement and mitigate the possible adverse effects of the infringement.[69]

84. The starting point for this assessment is that controllers and processors are expected to cooperate with the Commissioner in the performance of the Commissioner's tasks, for example by responding to requests for information and attending meetings.[70] The Commissioner considers that the ordinary duty of cooperation is required by law and meeting this standard is therefore not a mitigating factor.

85. However, the Commissioner may consider it appropriate to view cooperation as a mitigating factor where the controller or processor has responded to requests during the investigation in a way that:

- enables the enforcement process to be concluded significantly more quickly or effectively; or
- significantly limits the harmful consequences for people's rights and freedoms that might otherwise have occurred.

86. By contrast, the Commissioner may view persistent and repeated behaviour that delays regulatory action as an aggravating factor. Examples of such behaviour include not engaging with the Commissioner during the investigation or repeatedly failing to meet deadlines set by the Commissioner without reasonable excuse.[71]

The manner in which the infringement became known to the Commissioner

87. The Commissioner will have regard to the manner in which the infringement became known to the Commissioner, in particular whether, and if so to what extent, the controller or processor notified the Commissioner of the infringement.[72]

88. The Commissioner may view a controller or processor bringing an infringement to the Commissioner's attention of its own volition as a mitigating factor. This applies if the Commissioner was not already aware of the infringement.

89. However, this factor is not relevant if a controller or processor is under a statutory duty to comply with notification obligations in the UK GDPR or

[69] Article 83(3)(f) UK GDPR and section 155(3)(f) DPA 2018.
[70] Article 31 UK GDPR.
[71] Depending on the circumstances, the Commissioner may alternatively consider that such lack of cooperation is evidence that a person has failed to comply with an information notice, assessment notice or enforcement notice in breach of section 155(1)(b) DPA 2018.
[72] Article 83(3)(h) UK GDPR and section 155(3)(h) DPA 2018.

Part 3 or Part 4 DPA 2018.[73] The Commissioner will not consider notifications required by law, even if made promptly, as a mitigating factor. The Commissioner expects controllers and processors to comply with their statutory obligations.

90. Otherwise, the way in which the Commissioner finds out about an infringement – for example following a complaint, media coverage or through the Commissioner's own intelligence – will generally be considered as neutral.

Measures previously ordered against the controller or processor

91. Where measures referred to in Article 58(2) UK GDPR have previously been ordered against the controller or processor concerned with regard to the same subject-matter, the Commissioner will have regard to compliance with those measures.[74]

92. If a controller or processor has failed to comply with measures previously ordered under Article 58(2) UK GDPR concerning the same subject matter, the Commissioner may consider this to be either an aggravating factor or, if the controller or processor has failed to comply with an enforcement notice or penalty notice, as a separate infringement.[75] The Commissioner will take a similar approach under Part 3 and Part 4 DPA 2018, if a controller or processor has failed to comply with a previous enforcement notice or penalty notice.

Adherence to approved codes of conduct or certification mechanisms

93. The Commissioner will have regard to adherence to approved codes of conduct pursuant to Article 40 UK GDPR or approved certification mechanisms pursuant to Article 42 UK GDPR.[76]

94. Where a controller or processor has signed up to an approved code of conduct, the Commissioner will consider whether any action taken by a monitoring body in relation to a failure to comply with requirements covered by the code of conduct is sufficient without the Commissioner also issuing a penalty notice. However, the power of monitoring bodies to take

[73] See Article 33 UK GDPR, section 67 DPA 2018, and section 108 DPA 2018. Notification of a personal data breach does not necessarily imply that a controller or processor has infringed UK GDPR or Part 3 or Part 4 DPA 2018.

[74] Article 83(3)(i) UK GDPR. The measures referred to in Article 58(2) UK GDPR are set out at footnote 48. In relation to Part 3 and Part 4 DPA 2018, section 155(3)(i) contains a similar factor, but refers only to 'the extent to which the controller or processor has complied with previous enforcement notices or penalty notices'. Section 155(3)(i) is therefore not limited by such notices being required to relate to the 'same subject-matter'.

[75] As set out in section 115(8) DPA 2018, the Commissioner's powers under Article 58(2)(c) to (h) and (j) are exercisable only by giving an enforcement notice under section 149 DPA 2018. Similarly, the Commissioner's powers under Article 58(2)(i) and Article 83 UK GDPR are exercisable only by giving a penalty notice under section 155 DPA 2018 (see section 115(9) DPA 2018).

[76] Article 83(3)(j). The equivalent provision in section 155(3)(j) DPA 2018 simply refers to 'adherence to approved codes of conduct or certification mechanisms'.

appropriate action is without prejudice to the tasks and powers of the Commissioner.[77]

95. If a controller or processor has failed to comply with a code of conduct of which it is a member or meet the criteria of a certification mechanism directly relevant to the infringement, the Commissioner may consider this to be an aggravating factor. The Commissioner may also consider it as evidence relevant to whether the controller or processor's conduct is intentional or negligent.

Any other aggravating or mitigating factors

96. The Commissioner will have regard to any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained or losses avoided, directly or indirectly, from the infringement.[78]

97. Such factors may include:

- **Any economic or financial benefit obtained as a result of the infringement**. If a controller or processor profits from an infringement, the Commissioner is likely to give this significant weight as an aggravating factor. In order to be effective, proportionate and dissuasive, any fine should ensure that controller and processors are not in a position to make a profit or otherwise benefit financially from infringing data protection law. The Commissioner is therefore likely to investigate any economic or financial benefits that may have accrued to the controller or processor, including costs saved from any failure to invest in appropriate measures. The Commissioner recognises that in some cases it may not be possible to precisely quantify any such benefits.

- **Any action the controller or processor took pro-actively to report a cyber security breach to other appropriate bodies (such as the National Cyber Security Centre (NCSC)) and whether it followed any advice or guidance provided**. The Commissioner works with a range of other regulators and agencies, particularly in relation to cyber security matters. The Commissioner may give weight to a controller or processor's engagement and cooperation with another appropriate body as a mitigating factor, where that cooperation goes beyond what is required by law. The Commissioner expects the controller or processor to demonstrate and provide evidence of the steps it has taken to follow any such advice or guidance.[79] Reporting a security breach to another body is not a

[77] Article 40(4) UK GDPR.
[78] Article 83(3)(k) UK GDPR and section 155(3)(k) DPA 2018.
[79] For example, guidance on cyber security matters may include that provided by the NCSC, the National Institute of Standards and Technology (NIST) or the International Organisation for Standardisation (ISO). The

substitute for complying with an obligation to report personal data breaches to the Commissioner.

98. As explained in Calculation of the appropriate amount of the fine below, the Commissioner will also have regard to these aggravating and mitigating factors when deciding on the appropriate fine amount.

Effectiveness, proportionality and dissuasiveness

99. Section 155 DPA 2018 requires the Commissioner to consider whether issuing a penalty notice for an infringement is, in each case, effective, proportionate and dissuasive.[80]

100. In this context:

- 'Effective' means that imposing a fine achieves the objective of ensuring compliance with data protection legislation or providing an appropriate sanction for the infringement (or both).
- 'Proportionate' means that imposing a fine does not exceed what is appropriate and necessary in the circumstances to meet those objectives. In considering whether imposing a fine is proportionate, the Commissioner will take into account all the relevant circumstances, including:
  - the seriousness of the infringement;
  - the harm or other impact on data subjects; and
  - the controller or processor's size and financial position.
- 'Dissuasive' means that imposing a fine is a genuine deterrent to future non-compliance. The intention behind ensuring fines are 'dissuasive' is to promote compliance with data protection legislation. There are two aspects to deterrence in this context. First, there is a need to deter the controller or processor that is the subject of the fine from engaging in same infringing conduct again (referred to as 'specific deterrence'). Second, there is a need to deter others from committing the same infringement in the future (referred to as 'general deterrence').

101. The Commissioner's decision about whether to issue a penalty notice is a matter of evaluation and judgement. There is a degree of overlap between

extent to which a controller or processor has complied with such guidance is also likely to be relevant to whether there has been an infringement of the UK GDPR or Part 3 or Part 4 DPA 2018. However, whether or not an infringement has occurred in a particular case will depend on the assessment of all the relevant circumstances.

[80] In relation to UK GDPR see section 155(2)(a) and Article 83(1) UK GDPR; in relation to Part 3 and Part 4 DPA 2018 see section 155(3)(l) DPA 2018.

the concepts of effectiveness, proportionality and dissuasiveness. In making the decision, the Commissioner will first consider whether issuing a penalty notice is effective and dissuasive, before then considering whether it is proportionate to do so. As explained in Calculation of the appropriate amount of the fine below, the Commissioner will also have regard to effectiveness, proportionality and dissuasiveness in deciding on the appropriate fine amount.

102. The Commissioner will, in particular, consider the importance of imposing a fine only when it is needed and that any action taken is proportionate. In considering whether issuing a penalty notice and the fine amount is effective, proportionate and dissuasive, the Commissioner will have regard to the desirability of promoting economic growth, as required under section 108 of the Deregulation Act 2015. However, the Commissioner is mindful that the growth duty does not legitimise non-compliance with data protection law.[81] Non-compliant activity or behaviour undermines protections to the detriment of people as both data subjects and consumers. It also harms the interests of legitimate businesses that are working to comply with data protection law, which disrupts competition and acts as a disincentive to invest in compliance.[82]

[81] Department for Business, Energy & Industrial Strategy, Growth Duty: Statutory Guidance under section 110(6) of the Deregulation Act 2015, paragraph 1.5.
[82] Department for Business, Energy & Industrial Strategy, Growth Duty: Statutory Guidance under section 110(6) of the Deregulation Act 2015, paragraph 1.4.

Calculation of the appropriate amount of the fine

103. If the Commissioner decides to issue a penalty notice, the fine amount will be calculated by applying the following five step approach:

- **Step 1**: Assessment of the seriousness of the infringement.
- **Step 2**: Accounting for turnover (where the controller or processor is part of an undertaking).
- **Step 3**: Calculation of the starting point having regard to the seriousness of the infringement and, where relevant, the turnover of the undertaking.
- **Step 4**: Adjustment to take into account any aggravating or mitigating factors.
- **Step 5**: Assessment of whether the fine is effective, proportionate and dissuasive.

104. This approach is not intended to be mechanistic. The overall assessment of the appropriate fine amount involves evaluation and judgement, taking into account all the relevant circumstances of the individual case. The guidance sets out details about each of the steps below.

105. Having calculated the appropriate fine amount, in exceptional circumstances the Commissioner may reduce the fine where a controller or processor is unable to pay the proposed fine because of its financial position. The Commissioner's approach to claims of financial hardship is explained the section on Financial hardship below.

Step 1: Assessment of the seriousness of the infringement

106. The Commissioner will determine a starting point for the fine based on the seriousness of the infringement. The Commissioner will categorise the infringement according to its degree of seriousness and apply a starting point based on a percentage of the relevant applicable statutory maximum.

107. The Commissioner will use the following categories to determine the starting point:

- for infringements that have a high degree of seriousness, the Commissioner will use a starting amount of between 20% and 100% of the relevant legal maximum;
- for infringements that have a medium degree of seriousness, the Commissioner will use a starting point of between 10% and 20% of

the relevant legal maximum; and

- for infringements that have a lower degree of seriousness, the Commissioner will use a starting point of between 0% and 10% of the relevant legal maximum.

108. There is no pre-set 'tariff' of starting point for different types of infringement, given the range of conduct that may infringe the UK GDPR or DPA 2018. This is a case-specific assessment that, based on the guidance about the Commissioner's approach to seriousness set out above, will take into account:

the nature, gravity and duration of the infringement;

whether it was intentional or negligent; and

the categories of personal data affected.

109. As a general rule, the more serious an infringement, the more likely the Commissioner is to choose a higher starting point within the relevant category. The percentage range for infringements that have a high degree of seriousness is wider than those for infringements with a medium or lower degree of seriousness. This is to allow the Commissioner greater flexibility in deciding on the appropriate fine for more serious infringements. It also recognises that infringements with a lower or medium degree of seriousness are unlikely to warrant a starting point exceeding 10% or 20% of the relevant legal maximum respectively. The Commissioner will keep these percentage ranges under review as this guidance is applied in practice.

110. Where an undertaking's total worldwide annual turnover exceeds £435 million (in relation to the standard maximum amount) or £437.5 million (in relation to the higher maximum amount), the Commissioner will calculate the range for the starting point at Step 1 by reference to the turnover-based percentage figure specified as the relevant statutory maximum. In all other cases, the Commissioner will calculate the range for the starting point at Step 1 as a percentage of the fixed amount specified as the relevant statutory maximum.

111. The Commissioner will express the assessment of the level of seriousness at Step 1 as a percentage of the relevant statutory maximum applicable to the infringement. For example, the Commissioner may decide that an infringement falling within the high degree of seriousness category warrants a starting point of 40% of the higher maximum amount (falling within the 20% to 100% range). In that example, for a controller or processor to which the fixed amount applies, this would in practice equate to a starting point of £7 million (40% of £17.5 million).

112. For ease of reference, the way in which the Commissioner will apply the starting point to the standard maximum amount and the higher maximum amount is set out in **Table A** below.

Table A: Application of the starting point at Step 1 based on the standard maximum amount or higher maximum amount

	Lower degree of seriousness		Medium degree of seriousness		High degree of seriousness	
	Fixed amount	Turnover based	Fixed amount	Turnover based	Fixed amount	Turnover based
Standard maximum amount	Up to £870,000	Up to 0.2% of turnover	£870,000 to £1.74 million	0.2% to 0.4% of turnover	£1.74 million to £8.7 million	0.4% to 2% of turnover
Higher maximum amount	Up to £1.75 million	Up to 0.4% of turnover	£1.75 million to £3.5 million	0.4% to 0.8% of turnover	£3.5 million to £17.5 million	0.8% to 4% of turnover

Step 2: Accounting for turnover

113. The statutory maximum fine amounts that the Commissioner may impose under the UK GDPR and DPA 2018 apply across the full range of controllers and processors. This covers small businesses to multi-national corporations, as well as public bodies and not-for-profit organisations.

114. Therefore, the Commissioner considers that it is appropriate to take into account the turnover of an undertaking when assessing the starting point for the fine. This is consistent with the need to ensure that the amount of any fine is effective, proportionate and dissuasive.[83]

115. For undertakings, the Commissioner will first determine the undertaking's total worldwide annual turnover in its previous financial year. The Commissioner will then consider whether to adjust the starting point to reflect the size of the undertaking. The Commissioner will decide whether to exercise discretion to reduce the starting point in this way on a case-by-case basis, having regard to the circumstances of the infringement.

116. Where a controller or processor is not an undertaking and therefore does not have turnover, the Commissioner may instead have regard to other

[83] See EDPB, Binding Decision 1/2021, WhatsApp Ireland, paragraphs 411 and 412: '[Insofar] the turnover of an undertaking is not exclusively relevant for the determination of the maximum fine amount in accordance with Article 83(4)-(6) GDPR, but it may also be considered [as one relevant element among others] for the calculation of the fine itself, where appropriate, to ensure the fine is effective, proportionate and dissuasive in accordance with Article 83(1) GDPR'.

indicators of its financial position, such as assets, funding or administrative budget.[84]

Determination of total worldwide annual turnover

117. As explained in The concept of an 'undertaking' for the purpose of imposing fines above, an undertaking refers to any entity that is engaged in economic activity, regardless of its legal status or the way in which it is financed.

118. The relevant turnover of the undertaking for the purpose of calculating the maximum amount of the fine is the total worldwide annual turnover in its previous financial year.[85] In this context, the Commissioner considers that 'turnover' means the amount derived from the provisions of goods or services after deduction of trade discounts, value added tax and any other relevant taxes.[86]

119. An undertaking's previous financial year is the undertaking's financial year preceding the date of the Commissioner's decision (the date of the penalty notice). If a turnover figure is not available for that financial year, then the Commissioner will use the turnover figure for the financial year immediately preceding it.

120. The Commissioner will generally base turnover figures used for the purpose of calculating the fine on the consolidated turnover recorded in an undertaking's audited accounts.[87] However, there may be instances where the undertaking's audited accounts are not yet available (for example, if the Commissioner's decision to impose a fine closely follows the end of the undertaking's financial year and accounts for that financial year are not yet completed). If this is the case, the Commissioner will use the turnover figure from the audited accounts for the financial year immediately preceding it. The Commissioner may adjust the turnover figure used to ensure it reflects the true scale of the undertaking (for example, by using more recent management accounts or forecast figures, where available).

121. Where an undertaking does not have audited accounts, for example where it is exempt from audit requirements because it is a micro or small enterprise, the Commissioner will instead use the undertaking's unaudited accounts or other available financial information.

[84] In addition, as set out in Recital 150 UK GDPR, where a fine is imposed on a person that is not an undertaking, the Commissioner will, were relevant, take account of the general level of income in the UK as well as the economic situation of the person in considering the appropriate amount of the fine.
[85] See Article 83(4) to (6) UK GDPR and section 155(5) and (6) DPA 2018.
[86] See section 474 Companies Act 2006. The Commissioner will also have regard to relevant legislation relating to the calculation of 'turnover' that may arise for certain undertakings, for example in the areas of credit, financial services and insurance.
[87] In many cases, the most straightforward way to identify turnover for the undertaking will be to use the corporate group's consolidated financial accounts.

122. If necessary, the Commissioner will obtain financial information using the statutory power to issue information notices under section 142 DPA 2018. However, there may still be situations where the Commissioner can only obtain limited evidence. In such cases, the Commissioner may exercise judgement as to the appropriate turnover amount to use in calculating the fine.

Adjustment to reflect the size of the undertaking

123. As explained above, the Commissioner considers that it is appropriate to take into account the size of the undertaking when deciding on the starting point for the calculation of the fine.

124. In order to distinguish between undertakings, the Commissioner uses the following ranges set out in **Table B** below to determine an appropriate starting point that reflects their different sizes and financial positions, using turnover as a proxy. The ranges for micro-, small- and medium-enterprises (SMEs) are derived from the definition of SMEs used by the UK government.[88]

Table B: Ranges for adjustment based on the turnover of the undertaking

Annual turnover of the undertaking	Range for adjustment based on turnover of the undertaking
Up to £2 million (micro-enterprise)	Between 0.2% and 0.4%
£2 million to £10 million (small-enterprise)	Between 0.4% and 2%
£10 million to £50 million (medium-enterprise)	Between 2% and 10%
£50 million to £100 million	Between 10% and 20%
£100 million to £250 million	Between 20% and 50%
£250 million to £435 million[89] / £437.5 million[90]	Between 50% and 100%
Above £435 million / £437.5 million	No adjustment to the starting point[91]

[88] For example, see Department of Business, Energy and Industrial Strategy (now Department of Business and Trade), Small and medium enterprises (SMEs) action plan: 2022 to 2025 , which uses the European Commission definition of SMEs: SME definition. The European Commission's definition is derived from Article 2 of the European Commission's Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, (2003/361/EC). The Commissioner considers it is appropriate and clearer to apply these ranges in Pounds Sterling, rather than converting the amounts from Euros.

[89] Where the standard maximum amount applies.

[90] Where the higher maximum amount applies.

[91] Above £435 million (for the standard maximum amount) and above £437.5 million (for the higher maximum amount) the undertaking's size is already reflected by the use of a percentage figure to calculate the statutory maximum and the Commissioner will consider whether it is appropriate to impose a penalty up to the amount allowed by law.

125. As a general rule, the Commissioner is likely to choose a higher amount for undertakings with higher turnover within the applicable range. However, these ranges are only indicative. The Commissioner will reach a decision on a case-by-case basis as to whether it is appropriate to adjust the starting point of the fine in this way, having regard to the need for the fine to be effective, proportionate and dissuasive. Therefore, the Commissioner retains the discretion to impose a fine up to the applicable statutory maximum. If relevant, the Commissioner will give reasons for not making an adjustment at Step 2 based on the ranges set out in Table B.

126. The Commissioner will express any adjustment made to the starting point for the fine to reflect the size of an undertaking as a percentage based on the ranges set out in Table B.

Step 3: Calculation of the starting point

127. At Step 3, the Commissioner will calculate the starting point of the fine based on the outcomes of Step 1 and Step 2 as follows:

- Where the statutory maximum is a fixed amount:

statutory maximum amount (fixed) x adjustment for seriousness x turnover adjustment

Where the statutory maximum is turnover based:

turnover x statutory maximum amount (percentage) x adjustment for seriousness

128. **Table C** and **Table D** below set out the ranges of starting point for fines up to the standard maximum amount and the higher maximum amount respectively.

Table C: Indicative ranges for fine starting points for standard maximum amount based on Step 1 and Step 2

Annual turnover	Lower degree of seriousness	Medium degree of seriousness	High degree of seriousness
£0 to £2 million (micro-enterprise)	Range of between 0.2% and 0.4% of identified starting point at Step 1		
	Up to £3,480	£1,740 to £6,960	£3,480 to £34,800
£2 million to £10 million (small-enterprise)	Range of between 0.4% and 2% of identified starting point at Step 1		
	Up to £17,400	£3,480 to £34,800	£6,960 to £174,000
£10 million to £50 million (medium-enterprise)	Range of between 2% and 10% of identified starting point at Step 1		
	Up to £87,000	£17,400 to £174,000	£34,800 to £870,000
£50 million to £100 million	Range of between 10% and 20% of identified starting point at Step 1		
	Up to £174,000	£87,000 to £348,000	£174,000 to £1.74 million
£100 million to £250 million	Range of between 20% and 50% of identified starting point at Step 1		
	Up to £435,000	£174,000 to £870,000	£348,000 to £4.35 million
£250 million to £435 million	Range of between 50% and 100% of identified starting point at Step 1		
	Up to £870,000	£435,000 to £1.74 million	£870,000 to £8.7 million
Above £435 million	No adjustment to the identified starting point at Step 1 based on annual turnover[92]		

[92] Above £435 million (for the standard maximum amount) the undertaking's size is already reflected by the use of a percentage figure to calculate the statutory maximum and the Commissioner will consider whether it is appropriate to impose a penalty up to the amount allowed by law.

Table D: Indicative ranges for fine starting points for higher maximum amount based on Step 1 and Step 2

Annual turnover	Lower degree of seriousness	Medium degree of seriousness	High degree of seriousness
£0 to £2 million (micro-enterprise)	Range of between 0.2% and 0.4% of identified starting point at Step 1		
	Up to £7,000	£3,500 to £14,000	£7,000 to £70,000
£2 million to £10 million (small-enterprise)	Range of between 0.4% and 2% of identified starting point at Step 1		
	Up to £35,000	£7,000 to £70,000	£14,000 to £350,000
£10 million to £50 million (medium-enterprise)	Range of between 2% and 10% of identified starting point at Step 1		
	Up to £175,000	£35,000 to £350,000	£70,000 to £1.75 million
£50 million to £100 million	Range of between 10% and 20% of identified starting point at Step 1		
	Up to £350,000	£175,000 to £700,000	£350,000 to £3.5 million
£100 million to £250 million	Range of between 20% and 50% of identified starting point at Step 1		
	Up to £875,000	£350,000 to £1.75 million	£700,000 to £8.75 million
£250 million to £437.5 million	Range of between 50% and 100% of identified starting point at Step 1		
	Up to £1,750,000	£875,000 to £3.5 million	£1.75 million to £17.5 million
Above £437.5 million	No adjustment to the identified starting point at Step 1 based on annual turnover[93]		

[93] Above £437.5 million (for the higher maximum amount) the undertaking's size is already reflected by the use of a percentage figure to calculate the statutory maximum and the Commissioner will consider whether it is appropriate to impose a penalty up to the amount allowed by law.

129. As explained above, these ranges based on annual turnover are indicative. The Commissioner will reach a decision on a case-by-case basis as to whether it is appropriate to adjust the starting point of the fine in this way. In doing so, the Commissioner will have regard to the need for the fine in each individual case to be effective, proportionate and dissuasive.

130. To illustrate how the starting point would be calculated in practice, this guidance sets out two examples below. The first example covers an infringement with a medium degree of seriousness committed by a small enterprise. The second example covers an infringement with a high degree of seriousness committed by a large undertaking with more than £437.5 million turnover.

Example A

Step 1: An undertaking commits an infringement with a medium degree of seriousness. The Commissioner considers that the infringement warrants a starting point of 16% of the relevant legal maximum. The relevant legal maximum for the infringement in this case is the higher maximum amount (£17.5 million or 4%). Therefore, without any further adjustment, a fine based on the starting point at Step 1 would be either £2.8 million[94] (if the fixed amount applies) or 0.64% of turnover[95] (if the turnover based amount applies).

Step 2: The undertaking's turnover is £30 million. The Commissioner may therefore make an adjustment at Step 2 to reflect the size of the undertaking. As set out in Table B, the range for adjustment based on turnover for a medium enterprise with turnover between £10 million and £50 million is between 2% and 10% of the identified starting point at Step 1. Taking into account the circumstances of the case, the Commissioner decides that an appropriate adjustment at Step 2 is 5%.

Step 3: Applying the seriousness starting point at Step 1 of 16% and making an adjustment at Step 2 of 5% leads to a fine amount at the end of Step 3 of £140,000.

Statutory maximum amount (fixed) x Adjustment for seriousness x Turnover adjustment £17.5 million x 16% x 5% Starting point = £140,000

[94] £17.5 million x 16% = £2.8 million.
[95] 4% x 16% = 0.64%.

Example B

Step 1: An undertaking commits an infringement with a high degree of seriousness. The Commissioner considers that the infringement warrants a starting point of 40% of the relevant legal maximum. The relevant legal maximum for the infringement in this case is the higher maximum amount. Therefore, without any further adjustment, a fine based on the starting point at Step 1 would be either £7 million[96] (if the fixed amount applies) or 1.6% of turnover[97] (if the turnover-based amount applies).

Step 2: The undertaking's turnover is £800 million. The Commissioner may therefore decide not to make an adjustment at Step 2 to the identified starting point at Step 1 as the undertaking's size is already reflected in the fine calculation. This is because the turnover-based percentage figure of 4% for the higher maximum amount applies (the undertaking's turnover is above £437.5 million).

- **Step 3**: Applying the higher maximum amount turnover-based percentage (4%) and the seriousness starting point at Step 1 of 40% to the undertaking's turnover identified at Step 2 of £800 million leads to a fine at the end of Step 3 of £12.8 million.

Turnover x Statutory maximum amount (percentage) x Adjustment for seriousness
£800 million x 4% x 40%
Starting point = £12.8 million

Step 4: Aggravating and mitigating factors

131. At Step 4, the Commissioner will take into account whether there are any relevant aggravating or mitigating factors. These factors may warrant an increase or decrease in the level of the fine calculated at the end of Step 3.

132. The Commissioner will carry out a case-by-case assessment, based on the circumstances of the infringement, to decide whether the fine should be increased or reduced at Step 4. In carrying out this assessment, the Commissioner will have regard to the guidance on relevant aggravating or mitigating factors set out in Relevant aggravating or mitigating factors above.

133. An increase or decrease in the fine at Step 4 may lead to a fine amount that is above or below the relevant indicative range for the starting point of

[96] £17.5 million x 40% = £7 million.
[97] 4% x 40% = 1.6%.

the fine based on a controller or processor's turnover (see Steps 2 and 3 above). The Commissioner retains the discretion to use the full amount of the statutory maximum fine available, taking into account the circumstances of each individual case. However, the Commissioner will then consider whether any adjustment is necessary at Step 5 to ensure the fine is effective, proportionate and dissuasive.

Step 5: Adjustment to ensure the fine is effective, proportionate and dissuasive

134. As explained in Effectiveness, proportionality and dissuasiveness above, the Commissioner is required to ensure that any fine imposed for an infringement of UK GDPR or DPA 2018 is, in each case, effective, proportionate and dissuasive.

135. At Step 5, the Commissioner will therefore consider the circumstances of the case in the round to assess whether the fine reached at the end of Step 4 is appropriate. The Commissioner will adjust the amount of the fine at Step 5, if necessary, to ensure that:

the overall fine is effective, proportionate and dissuasive; and

it does not exceed the relevant statutory maximum amount.

136. Where the Commissioner has found that a controller or processor has infringed more than one provision of the UK GDPR or DPA 2018 in relation to the same or linked processing operations (see The Commissioner's approach to fines where there is more than one infringement by a controller or processor above), the Commissioner will assess the effectiveness, proportionality and dissuasiveness of:

the fine amount for each infringement calculated at the end of Step 4; and

the combined amount of the overall fine (ie the sum of the fine amounts imposed for each infringement).

Where the Commissioner considers that an adjustment is needed at Step 5 to ensure the fine is sufficiently dissuasive, the Commissioner may adjust the overall fine (rather than the amounts for each infringement).

By contrast, where the Commissioner has found that different forms of conduct by a controller or processor have infringed separate provisions of the UK GDPR or DPA 2018, the Commissioner will assess the effectiveness, proportionality and dissuasiveness of each fine separately.

Whether the fine amount is effective, proportionate and dissuasive

137. In carrying out the assessment, the Commissioner will be mindful that the aim of Steps 1 to 4 of the calculation is to identify a fine amount that is

effective, proportionate and dissuasive. The purpose of Step 5 is to provide the opportunity for the Commissioner check that is the case. It allows the Commissioner to increase or decrease the penalty as necessary, having regard to all the relevant circumstances of each individual case.

138. There is a degree of overlap between the concepts of effectiveness, proportionality and dissuasiveness. The Commissioner's decision on an appropriate fine amount is not a mechanistic assessment, but one of evaluation and judgement.

139. The Commissioner will first consider whether the fine amount at the end of Step 4 is effective in ensuring compliance with data protection legislation or providing an appropriate sanction for each infringement.

140. The Commissioner will then consider whether the fine amount is dissuasive, taking into account both 'specific deterrence' and 'general deterrence' (see Effectiveness, proportionality and dissuasiveness above):

For specific deterrence, the Commissioner may increase the overall fine reached after Step 4 to ensure that the amount is sufficient to deter the controller or processor from infringing data protection law in the future, taking into account its size and financial position, as well as any other relevant circumstances of the case. The Commissioner may impose a higher fine on a larger organisation than a smaller organisation for a similar infringement to achieve the necessary deterrent effect.

For general deterrence, the Commissioner may increase the overall fine reached after Step 4 to deter others from committing the same infringement in the future.

141. Finally, the Commissioner will consider whether the fine is proportionate. This assessment involves the exercise of the Commissioner's judgement and discretion, taking into account the nature and specific context of the infringement.

142. In reaching a decision on whether a fine is effective, proportionate and dissuasive, the Commissioner will have regard to all relevant circumstances of each individual case. This includes:

- the seriousness of the infringement;
- any aggravating or mitigating factors;
- the controller or processor's size and financial position; and

the need for effective deterrence.[98]

143. A controller or processor responsible for a serious infringement of UK GDPR or DPA 2018 should not avoid a fine solely on the basis of its financial position. This would undermine a key purpose of the legislation.[99] However, the Commissioner will consider an organisation or individual's financial hardship and ability to pay following the determination of an appropriate fine (see Financial hardship below).

144. This guidance ensures that the Commissioner adopts a consistent approach to calculating fines. It also provides flexibility to set the appropriate fine amount based on the specific facts and circumstances of each infringement. In assessing whether the fine is proportionate, the Commissioner will have regard to the level of fines set in previous cases, where relevant. However, the Commissioner is not bound by previous decisions. The Commissioner may, taking into account the individual circumstances of each case, impose higher fines in future cases than in previous ones, for example to ensure effective deterrence.

Adjustment to ensure that the statutory maximum amount is not exceeded

145. The final amount of the fine must not exceed the relevant statutory maximum amount. Therefore, the Commissioner will, as a final check, ensure that the fine does not do so and will decrease it if necessary.

Financial hardship

146. In exceptional circumstances, the Commissioner may reduce a fine where an organisation or individual is unable to pay because of their financial position. The organisation or person concerned needs to make a claim of financial hardship. They will have the burden of proving that their situation merits such a reduction.

147. The Commissioner will only grant a reduction for financial hardship on the basis of objective evidence that imposing the proposed fine would irretrievably jeopardise an organisation's economic viability or bankrupt an individual. The Commissioner will consider evidence about the organisation or individual's financial position (including cash flow and ability to borrow and, where relevant, dividends or other forms of value extracted from the organisation). The Commissioner will not base any reduction on the mere finding of an adverse or loss-making financial situation. The Commissioner

[98] The Commissioner will generally take into account an undertaking's total worldwide annual turnover as the primary indicator of its size and financial position. However, the Commissioner will also consider other financial indicators where relevant, such as profits, net assets or dividends.

[99] See *Doorstep Dispensaree Limited v Information Commissioner*, [2021] UKFTT (Information Rights), EA/2020/0065/V, 9 August 2021, paragraph 93. Upheld on appeal: see *Doorstep Dispensaree Limited v Information Commissioner*, [2023] UKUT 132 (AAC).

will also take into account that there may be circumstances where a fine may be effective, dissuasive and proportionate even if the controller or processor is unable to pay and is rendered insolvent.

148. Where appropriate, the Commissioner may enter an agreement providing additional time to pay a fine or to allow for the payment of the fine in instalments. The Commissioner will only reduce a fine for financial hardship in circumstances where such a reduction is merited in addition to any agreed payment plan.

Annex 1: Table setting out the relevant provisions of UK GDPR and DPA 2018 in relation to which the Commissioner can impose a fine under section 155(1) DPA 2018

	UK GDPR	Part 3 DPA 2018: Law Enforcement processing	Part 4 DPA 2018: Intelligence Services processing
The principles of processing	✓ Articles 5-11	✓ Sections 34-42	✓ Sections 85-91
Data subject rights	✓ Articles 12-22	✓ Sections 43-54	✓ Sections 92-100
Obligations imposed on controllers or processors	✓ Articles 25-39	✓ Section 64 or Section 65	✗
The requirement to communicate a personal data breach to the Commissioner or a data subject	✓ Articles 33-34	✓ Section 67 or Section 68	✓ Section 108
The principles for transfers of personal data to third countries, non-Convention countries and international organisations	✓ Articles 44-49	✓ Sections 73-78	✓ Sections 73-78
Specific failures of a monitoring body (monitoring approved code of conduct)[100]	✓	N/A	N/A
Specific failures of a certification provider[101]	✓	N/A	N/A
A failure to comply with regulations under section 137 DPA 2018	✓	✓	✓

[100] s149(3) DPA 2018: Where the monitoring body has failed, or is failing, to comply with an obligation under Article 41 UK GDPR.

[101] s149(4) DPA 2018: Where a certification provider does not meet the requirements for accreditation; has failed, or failing, to comply with an obligation under Articles 42 or 43 UK GDPR; or has failed or is failing to comply with any other provision of the UK GDPR (whether in the person's capacity as a certification provider or otherwise).

A failure to comply with the terms of an information notice, assessment notice or enforcement notice[102]	✓	✓	✓

[102] s155(1)(b) DPA 2018

Annex 2: Table setting out the relevant provisions of UK GDPR and DPA 2018 to which the standard maximum amount and higher maximum amount apply

Standard maximum amount

	UK GDPR provision[103]	Part 3 DPA: Law Enforcement processing [104]	Part 4 DPA: Intelligence Services processing [105]
Obligations of controller and processor	Articles 8, 11, 25-39, 42	Sections 64-65 and Sections 67-68	Section 108
Obligations of the certification body	Articles 42 and 43	N/A	N/A
Obligations of the monitoring body	Article 41(4)	N/A	N/A

Higher maximum amount

	UK GDPR provision[106]	Part 3 DPA: Law Enforcement processing [107]	Part 4 DPA: Intelligence Services processing[108]
The basic principles for processing, including conditions for consent	Articles 5,6,7 and 9	Sections 35-37, Section 38(1), Section 39(1), Section 40	Sections 86-91
Data subject rights	Articles 12-22	Sections 44-49 and Sections 52-53	Sections 93-94 and Section 100
Transfers of personal data to a recipient in a third country or an international organisation	Articles 44-49	Section 73 and Sections 75-78	Section 109

[103] Art 83(4)
[104] s157(2)
[105] s157(3)
[106] Art 83(5)
[107] s157(2)
[108] s157(3)

Non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the Commissioner	Article 58(2)(f) and Article 58(2)(j)	Section 157(4)	Section 157(4)
Failure to comply with an information notice, assessment notice or enforcement notice	Article 58(5)(e) and Article 58(6)[109]	Section 157(4)	Section 157(4)

[109] See also section 157(4) DPA 2018.

E03080084

978-1-5286-4719-9