DRAFT

Data protection enforcement procedural guidance

Data Protection Act 2018 and UK General Data Protection Regulation

31 October 2025

ico.
Information Commissioner's Office

Contents

1 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 explains how the Commissioner generally conducts investigations and takes enforcement action using the powers set out in the UK GDPR and the DPA 2018.

3. As a corporation sole, all formal powers and duties under the UK GDPR and the DPA 2018 rest with the Commissioner. In practice, the Commissioner is supported by the Information Commissioner's Office (ICO). ICO staff act under delegated authority from the Commissioner. Where this guidance refers to 'ICO', 'we' or 'our' in the context of taking action under the UK GDPR or the DPA 2018 it should, where relevant, be understood as a reference to the Commissioner taking action.

1.1 The scope of this guidance

4. This guidance is primarily aimed at controllers or processors that process personal data within the scope of the UK GDPR and the DPA 2018. In the context of this guidance, we refer to the UK GDPR and the DPA 2018 together as the "data protection legislation". The guidance may also be of interest to others who want to understand how we use some of our statutory powers to investigate and enforce data protection legislation.

5. This guidance sets out how we normally approach our investigations and take enforcement action where we suspect that a controller or processor has failed, or is failing, to comply with its obligations under data protection legislation.

6. The ICO's investigatory and enforcement powers are set out in article 58 UK GDPR and Part 6 of the DPA 2018.[1] These powers enable us to obtain information, assess compliance and, where necessary, take enforcement action against controllers or processors that infringe data protection legislation.[2]

7. In summary, our investigatory and enforcement powers include:

    - requiring controllers or processors and others to provide information and documents[3];

[1] Other general functions of the ICO relating to Part 3 and Part 4 DPA 2018 are set out in schedule 13 DPA 2018 and schedule 15 DPA 2018 sets out the ICO's powers of entry and inspection. Note that the ICO's functions under article 58 UK GDPR are subject to the safeguards set out in section 115 DPA 2018.
[2] In certain circumstances we may also take enforcement action in relation to monitoring bodies or certification providers under section 149(3) and (4) DPA 2018.
[3] Section 142 DPA 2018 (information notices).

- conducting assessments of a controller or processor's compliance with data protection legislation, including by entering its premises and requiring reports by approved persons;[4]
- requiring individuals to attend interviews and answer questions;[5]
- entering and inspecting premises under warrant;[6]
- giving a warning to a controller or processor if its intended processing operations are likely to infringe data protection legislation;[7]
- giving a reprimand to a controller or processor if its processing operations have infringed data protection legislation;[8]
- giving an enforcement notice to order a controller or processor to take appropriate steps to remedy an infringement; or
- imposing a fine by giving a penalty notice.[9]

8. When carrying out our functions under the UK GDPR and the DPA 2018 and deciding what regulatory action to take, we must take into account our principal objective to:

- secure an appropriate level of protection for personal data, having regard to the interests of data subjects, controllers and others and matters of general public ; and
- promote public trust and confidence in the processing of personal data.[10]

9. When deciding on the appropriate action to take, we also consider the desirability of promoting economic growth and our other statutory duties as are relevant in the circumstances[11], as well as our duty as a public body to act fairly and reasonably.

10. This guidance does not apply to prosecuting criminal offences under the DPA 2018. However, it provides statutory guidance on the information

[4] Section 146 DPA 2018 (assessment notices) and section 129 DPA 2018 (consensual audits).
[5] Section 148A DPA 2018 (interview notices).
[6] Section 154 and schedule 15 DPA 2018.
[7] Article 58(2)(a) UK GDPR and paragraph 2(b), schedule 13 DPA 2018.
[8] Article 58(2)(b) UK GDPR and paragraph 2(c), schedule 13 DPA 2018.
[9] Section 155 DPA 2018. See also the ICO's Data Protection Fining Guidance.
[10] Section 120A DPA 2018.
[11] As required by section 108 Deregulation Act 2015 and section 120B DPA 2018, which refers to the desirability of promoting innovation; the desirability of promoting competition; the importance of the prevention, investigation, detection and prosecution of criminal offences; the need to safeguard public security and national security; and the fact that children merit specific protection with regard to their personal data because they may be less aware of the risks and consequences associated with processing of personal data and of their rights in relation to such processing.

gathering powers we may use to investigate either a potential infringement of data protection legislation or a criminal offence.[12]

1.2 The status of this guidance

11. This guidance applies to the use of our investigatory and enforcement powers under the DPA 2018 and the UK GDPR from the date of its publication.

12. We will keep the guidance under review. We may revise it from time to time to reflect changes in the law or our practices.

13. The guidance sets out our general approach to enforcement. This means that we will take this guidance into account when using our investigatory and enforcement powers. However, it is designed to be flexible and we may adopt a different approach where there are good reasons to do so in the specific circumstances of a case.

14. If we do depart from this guidance, we will explain our reasons for doing so and will always abide by our duty to act fairly and reasonably.

15. This guidance is not a definitive statement of, or a substitute for, the law itself. It should also be read alongside our other guidance on data protection, including the Data Protection Fining Guidance.[13]

16. Alongside the Data Protection Fining Guidance, this guidance fulfils our statutory obligation to publish guidance about regulatory action as set out in section 160 DPA 2018 and about privileged communications as set out in section 133 DPA 2018. It replaces our previous statutory guidance on regulatory action set out in the Regulatory Action Policy published in November 2018.[14]

2 How we decide whether to open an investigation

17. We have a broad range of tasks and powers under data protection legislation. This section focuses on the process we follow when deciding to open an investigation into whether a controller's or processor's processing of personal data has infringed data protection law and, if so, what action, if any, is appropriate. It explains how we gather information prior to opening an investigation, as well as the steps we may choose to take other than opening an investigation. It also explains that when we do decide to open

[12] For example, the offence of unlawfully obtaining personal data under section 170 DPA 2018 or the offence of re-identification of personal data under section 171 DPA 2018. For the ICO's criminal powers, see: ICO Prosecution policy statement, May 2018.
[13] Information Commissioner: Data Protection Fining Guidance, March 2024.
[14] Regulatory Action Policy (ico.org.uk).

an investigation, we will inform the controller or processor that we have done so.

18. When we refer to opening an investigation, this means that we have notified a controller or processor by sending it a case opening letter (see section 3.1 Opening an investigation). This does not include informal enquiries that may precede us opening an investigation or may be part of our policy or engagement work. It also does not include situations where we've received a complaint and we are considering the extent that it is appropriate for us to investigate its subject matter.[15]

19. We make decisions about how to use our regulatory powers on a case-by-case basis, taking into account our statutory duties and the specific circumstances of the case. We cannot open investigations into every complaint or personal data breach report we receive, and it would not be proportionate to do so. It is important that we use our resources in an efficient and effective way.

2.1 Sources of potential investigations

20. We receive information about potential infringements of data protection legislation from a wide range of sources, such as:

- complaints or other information from data subjects, civil society, controllers or processors, the public sector, or industry bodies;
- personal data breach reports or self-reported concerns from controllers or processors;
- reports in the media;
- information provided by whistleblowers;[16]
- information from other regulatory bodies; or
- our own research, monitoring, audits and engagement with controllers or processors.

21. We receive many thousands of complaints from people every year. In some cases, an individual complaint may result in us opening an investigation. For example, if the complaint provides evidence of a serious alleged infringement of data protection legislation.[17] Similarly, we receive

[15] Section 165(5)(a) DPA 2018. See: What to expect from the ICO when making a data protection complaint for further information about how we process complaints and the outcomes of complaints. However, complaints may lead to us opening an investigation.
[16] See further information about whistleblowing complaints: Protected disclosures to the ICO – Whistleblowing | ICO.
[17] Where the ICO receives a complaint from a data subject it must, among other things, take appropriate steps to respond to the complaint and inform the complainant of the outcome of the complaint (see section 165 DPA

thousands of personal data breach reports from controllers each year. It is important to recognise that notification of a personal data breach by a controller does not necessarily mean that the controller (or its processor) has infringed data protection legislation. However, a personal data breach report may lead to us opening an investigation.

22. We monitor trends in complaints and personal data breach reports to help identify particular areas of concern and allow us to focus on issues posing the greatest risk of harm to people. This enables us to prioritise making regulatory interventions based on the factors set out below. This includes opening investigations where we suspect an infringement and taking enforcement action if needed. In this way, we aim to make the best use of our resources and achieve the greatest impact.

2.2 The factors we consider when deciding to open an investigation

23. We consider a range of factors when deciding whether to open an investigation and what action to take, taking into account our duty as a public body to act fairly and reasonably.

24. The main factors we generally consider include:

- the risk of harm to people caused by the processing operations (referring, where appropriate, to our data protection harms taxonomy), and whether the conduct is ongoing[18];
- the scale of the actual or potential impact of the processing operations on people across the UK and whether regulatory intervention would help to protect the rights of people who need extra support to protect themselves;
- the extent to which opening an investigation would support economic growth and improve compliance, considering the need to deter similar conduct by others and protect the interests of controllers or processors that work hard to comply with data protection law;
- the extent to which opening an investigation supports our strategic objectives[19];
- the resource implications and risks involved in opening an investigation;

2018). Taking appropriate steps involves the ICO "investigating the subject matter of the complaint, to the extent appropriate". This does not require the ICO to open an investigation or use its statutory powers in respect of every complaint (see R (Delo) v Information Commissioner [2023] EWCA Civ 1141, paragraph 80). See also recital 141 UK GDPR.

[18] ICO, Overview of data protection harms and the ICO taxonomy, April 2022.

[19] The ICO's strategic objectives can be found in its Annual Reports, and the ICO25 Strategic Plan.

- whether the controller or processor has been subject to previous regulatory action, or if this conduct is repeated; and
- whether another regulator may be better placed to take action.

2.3 Information gathering

25. Before we open an investigation, we typically undertake information gathering to develop a view on the issues and the factors described previously. This helps us decide whether it is appropriate to open an investigation or take some other action. Where we decide not to act, we can nonetheless use complaints and personal data breaches to build up our understanding to inform future work.

26. When gathering information, we keep an open mind about whether there has been an infringement of data protection legislation. We assess whether any concerns we identified warrant us taking further action and, if so, what action may be appropriate. The level of detail and extent of our information gathering varies as we consider appropriate. This depends on the circumstances of the case, whether there is a need to take urgent action to protect people, and the complexity of the issue.

27. Before opening an investigation, we typically ask controllers or processors to provide information voluntarily. However, we may use our statutory powers in certain circumstances. For example, if it helps us to effectively prioritise our resources or support our work to determine whether to open an investigation. (See section 4.1 Information notices, section 4.2 Assessment notices and section 4.3 Interview notices.)

28. If we ask a controller or processor to provide us with information voluntarily, we usually do so in writing.

29. In some cases, we may request to meet with the controller, processor or third parties (such as a complainant) if we consider this will assist us in deciding whether to open an investigation. We expect controllers and processors to cooperate with us in line with their obligations under data protection legislation.[20] This includes ensuring that they provide accurate information to us in response to any questions we ask during our initial assessment.

30. In some circumstances, we may decide not to engage with a controller or processor when gathering information. For example, where:

    - we already have sufficient information to decide whether to open an investigation;

[20] See article 31 UK GDPR and section 63 DPA 2018.

- there are grounds to proceed to an investigation more quickly; or
- it might be important to safeguard the anonymity of a complainant.[21]

2.4 Potential outcomes following information gathering

31. Potential outcomes following information gathering include:

- opening an investigation;
- using means other than an investigation to seek to resolve the issue; or
- taking no further action.

2.4.1 Opening an investigation

32. The process that we follow when opening and conducting investigations, including the use of our statutory information gathering powers, is set out in sections 3 to 5 of this guidance. The potential outcomes of an investigation are explained in section 6. We decide what action is appropriate depending upon the circumstances of each investigation.

2.4.2 Other means of resolving the issue

33. If we decide not to open an investigation, we may seek to resolve the issue through other means. This may include taking one or more of the following steps:

- **Informing a controller or processor about our concerns:** We may inform a controller or processor that we have concerns about its compliance with data protection legislation. This does not necessarily mean that it has infringed data protection legislation, but it informs the controller or processor that we have concerns about the way it is processing people's information. We may also set out our views about how it could change its processing operations in order to ensure it complies with data protection legislation. Any failure by the controller or processor to take steps to address our concerns may lead to us deciding to open an investigation in the future.
- **Giving a warning if a controller or processor's intended processing operations are likely to infringe data protection legislation**: We have the power to give a warning to a controller or processor if we consider its intended processing operations are likely

[21] The ICO will consider requests from complainants to remain anonymous. Ideally, the complainant should request anonymity at the time of making their complaint. However, it may not be feasible to conduct our initial assessment, or take enforcement action, without revealing the identity of the complainant to the subject of the investigation. Additional considerations may apply to whistleblowers, see: Protected disclosures to the ICO – Whistleblowing.

to infringe data protection legislation.[22] If we subsequently find that the controller or processor commenced the intended processing, and committed an infringement, we may regard the failure to heed the warning as an aggravating factor when considering future enforcement action, including the amount of any fine. We may also give a warning after we have opened an investigation (see section 7 Process for giving warnings).

- **Providing advice and recommendations, publishing guidance, amending a statutory code of practice or giving an opinion**: We may provide advice or make recommendations about how a controller or processor could improve its practices. We may also suggest that it participates in an ICO audit.[23] Our information gathering may indicate that further guidance is required or that an amendment to a code of practice is needed. For example, to provide clarity for controllers or processors about how to comply with data protection legislation. If the information we gather highlights issues about processing personal data, we may decide it is important to set out our view in an opinion.[24]

- **Accepting assurances to remedy compliance concerns**: Before opening a formal investigation, we may engage with a controller or processor to give them opportunity to address or remedy any concerns we may have about their compliance. Instead of opening a formal investigation, we may agree to accept assurances from the controller or processor about steps it has taken or will shortly take to remedy our concerns. For example, this may include committing to implement measures to improve compliance, providing redress for any damage or distress people may have suffered, or agreeing to an audit by the ICO and publication of findings to promote best practice. We generally expect a controller or processor to give such assurances in writing, eg in the form of an undertaking, signed by a senior representative of the organisation. We expect to make such assurances public, and we will monitor the controller or processor's compliance with them.

- **Referring the issue to another public body that may be better placed to deal with it**: If it appears to us that another public body

[22] Article 58(2)(a) UK GDPR and paragraph 2(b), schedule 13 DPA 2018.
[23] The ICO can carry out consensual audits under section 129 DPA 2018. For further information, see: Audits | ICO.
[24] The ICO is able to give an opinion under article 58(3)(b) UK GDPR and section 115(3)(b) DPA 2018 in relation to the processing of personal data to which the UK GDPR applies. Opinions relating to Part 3 and Part 4 DPA 2018 processing can be given under paragraph 2(d), schedule 13 DPA 2018. The Commissioner's opinions are available on our website: Information Commissioner's Opinions | ICO.

or regulator would be better placed to deal with the matter, we will raise it with them.[25]

- **Making a statement to inform or educate people:** We may make a public statement to inform or educate people about particular information processing issues or practices that we identified during our information gathering.

34. If we do not open an investigation and seek to resolve the issue through other means, we generally do not take any decision about whether the controller or processor has infringed any data protection legislation. We may publicly announce any action we take if we have sought to resolve the issue through other means. If so, we usually inform the controller or processor before taking this step.

2.4.3 Taking no further action

35. We may decide not to open an investigation or take any other steps. This may be the case if:

- we do not consider any further action is warranted based on the available evidence;
- the scale of any harm appears too low to merit further action, or does not merit further action based on the factors we use to prioritise work;
- we are satisfied that a controller or processor has already taken appropriate steps to address any concerns we have identified, and we do not consider any further action is appropriate; or
- we consider that we are not best placed to act (eg we consider another public body is best placed to act or is already investigating the matter).

36. If we decide to take no further action, we usually inform the controller or processor about this outcome if we have previously asked it for information. We explain why we have decided not to open an investigation or take any further action. We may explain the circumstances in which we might reconsider opening an investigation in future. We may also inform any complainant about our decision. We always inform any complainant about the outcome of their complaint if it was about their personal data.[26]

37. We do not usually publicly announce a decision to take no further action after information gathering. However, we may make exceptions depending

[25] For example, this may include other regulators in the Digital Regulation Co-operation Forum (DRCF), namely the Competition and Markets Authority (CMA), the Financial Conduct Authority (FCA) and the Office of Communications (Ofcom).
[26] Section 165(4)(b) DPA 2018.

on the specific circumstances of the case. For example, if the issue we are considering is the subject of media speculation and we think we should clarify our position. If so, we usually inform the controller or processor in advance if we decide to publicly announce these details and give it a copy of our intended publication.

3 What to expect during an investigation

38. This section explains what to expect during an investigation. It summarises the process we generally follow, including when we make details of an investigation public.

3.1 Opening an investigation

39. If we open an investigation, it means we are satisfied the available evidence merits doing so and the issue is a priority. However, opening an investigation does not mean we have taken a view on whether a controller or processor has, or continues to, infringe data protection legislation.

40. The decision to open an investigation is taken by an individual within the ICO with the appropriate delegated authority, following consultation with other members of staff. Typically, this is a senior employee of the ICO and they oversee the investigation (the "senior leadership lead").

41. We establish a case team to be responsible for the day-to-day running of the investigation. The case team is led by a designated case lead who is the main point of contact for the controller or processor during the investigation. The case team draws on expertise from across the ICO as necessary during the investigation (eg from Legal Service, Economic Analysis, and Technology).

42. At the start of an investigation, we usually send the subject of the investigation a case opening letter. We typically send it in electronic form, via email.

43. The case opening letter sets out the following details:

- the name and contact details of the allocated point of contact (ie the case lead), and the senior leadership lead responsible for overseeing the investigation;
- the scope of the investigation, including the specific legal obligations imposed by data protection legislation that the investigation relates to and which we suspect the controller or processor has, or continues to, infringe;
- information about our information gathering and enforcement powers;
- details of any complaints, if appropriate (see section 5.3 Handling confidential information) and
- the next steps in the investigation and their estimated timeframe.

44. The case opening letter asks the controller or processor to nominate a principal point of contact for communications about the investigation.

45. Sending the case opening letter may coincide with the exercise of our information gathering powers. For example, we may send an information notice or an assessment notice at the same time as sending the case opening letter (see section 4 Information gathering).

46. We may delay sending a case opening letter, if it could prejudice our ability to carry out an effective investigation. For example, if we decide to use our powers of entry and inspection (see section 4.4 Powers of entry and inspection).

47. In some cases, we may already have sufficient information after making enquiries to reach a provisional decision that a controller or processor has, or continues to, infringe the UK GDPR or the DPA 2018. If so, we may give a notice of intent to give a penalty notice or a preliminary enforcement notice at the same time as, or soon after, sending the case opening letter. In particular, if we consider it is appropriate to impose an urgent enforcement notice (see section 9 Process for giving enforcement notices).

3.2 Announcing investigations

48. After the subject of the investigation has received the case opening letter, we generally announce on our website that we have opened an investigation. There may be exceptional cases where we consider it is inappropriate to announce we have opened an investigation. For example, if:

    - doing so could prejudice our ability to carry out our investigation;
    - the case is particularly sensitive; or
    - publicity could have a detrimental impact on third parties (such as any complainants or data subjects).

49. The information we publish on our website typically includes the identity of the controller or processor under investigation and a brief summary of the case. We also make a statement that the opening of the investigation should not be taken to mean that we have reached a conclusion that the controller or processor has, or continues to, infringe data protection law.

50. If the controller or processor is a named individual, we do not usually announce the investigation at this stage.

51. We do not agree the text of case opening announcements with the subject of the investigation. We provide it with the text of our statement in advance of publication to give it an opportunity to comment on factual inaccuracies or matters of confidentiality in the proposed text. If we consider the

circumstances require us to act with urgency, we may give a shorter period of notice or make an announcement without providing advanced notice.

52. If we consider an announcement to be potentially market sensitive, we generally inform the controller or processor about our intention to publish after the market in the UK has closed and publish at 7.00am on our website. If the controller or processor under investigation, or its parent company, is a listed company in another jurisdiction and the announcement is potentially market sensitive, we will, where possible, seek to avoid publication during stock exchange hours in that other jurisdiction.[27]

3.3 Engagement with the ICO during the investigation

53. We conduct the investigation in a fair, transparent, efficient and timely way. The time we take to establish the facts and decide whether there is an infringement varies from case-to-case. It depends on a range of factors, such as the complexity of the processing under investigation and the extent that the controller or processor cooperates with us.[28]

54. If our assessment of the information (see section 4 Information gathering) indicates that a controller or processor has infringed, or continues to infringe, data protection legislation, we consider whether to give a:

- preliminary enforcement notice; or
- notice of intent to give a reprimand or penalty notice.

55. These notices are a provisional decision setting out our provisional findings of infringement and reasons why we are proposing to take enforcement action.

56. If we consider that a controller or processor's intended processing operations are likely to infringe data protection legislation, then we may give a warning. As explained previously, we may give a warning without opening an investigation (see section 7 Process for giving warnings).

57. We generally provide updates on the progress of the investigation by telephone or in writing. However, if we are considering proceeding to give a notice of intent to impose a penalty notice, we typically offer the controller or processor under investigation an opportunity to meet with representatives from the case team before doing so (either in person or at a virtual meeting). At this meeting, we provide our provisional thinking on the case, including outlining the concerns we have identified.

[27] This will include, where possible, avoiding publication during any extended trading hours on the exchange on which the subject of the investigation is listed.
[28] Article 31 UK GDPR and section 63 DPA 2018 require controllers and processors to cooperate with the ICO in the performance of our tasks.

58. We may also offer to meet at this stage of the investigation if we are considering giving a preliminary enforcement notice. We decide whether it is appropriate to do so on a case-by-case basis, depending upon the nature of the investigation and the requirements we intend to impose.

59. We generally only offer to meet before giving a notice of intent to impose a reprimand if there are exceptional circumstances that mean it is necessary in the interests of fairness.

60. The recipient of a preliminary enforcement notice or notice of intent has an opportunity to make representations in writing. In some cases, it also has an opportunity to attend a hearing to make oral representations. Further information is set out in sections 7 to 10 about the opportunity to make representations about warnings, reprimands, enforcement notices and penalty notices.

61. Having considered any representations, we decide whether it is appropriate to confirm our findings and take enforcement action. We may decide not to take enforcement action at this stage, if we consider that:

    - there is insufficient evidence of an infringement;
    - the issue could be resolved through other means; or
    - the matter is no longer a priority (see section 2.4 Potential outcomes following information gathering).

3.4 Changing the scope of an investigation

62. As previously explained, we set out the scope of the investigation in the investigation opening letter. We may widen the scope of an investigation if we identify new areas of concern that merit investigation or reduce the scope if it becomes apparent that it is no longer appropriate to pursue aspects of a case.

63. If we change the scope of an investigation, we inform the subject of the investigation and, if necessary, update our website.

3.5 Involvement of third parties

64. In some cases, third parties (including complainants) may be directly affected by the outcome of an investigation. They can also play a valuable role in an investigation by drawing issues to our attention and providing us with relevant information.

65. We involve third parties in an investigation to the extent that we consider it appropriate in order to carry out our functions fairly, transparently and effectively. We may engage with complainants during the course of an

investigation, including providing them with updates and information about progress.

3.6 How to raise concerns about the investigation process

66. If the subject of an investigation is unhappy about our procedures or handling of the case after we have opened an investigation, it should raise its concerns with the case lead or senior leadership lead.

67. Otherwise, it should follow our complaints policy to make any complaints about our service.[29]

4 Information gathering

68. We have a range of information gathering powers under the DPA 2018 to help us carry out our functions. This includes obtaining evidence to establish whether a controller or processor has complied, or is complying, with data protection legislation and to decide on the appropriate enforcement action, where necessary.

69. These powers include:

- giving information notices to obtain information and documents;
- giving an assessment notice that requires a controller or processor to allow us to carry out an assessment of whether they are complying with data protection law;
- giving an interview notice that requires an individual to attend an interview and answer questions; and
- powers of entry and inspection.

70. In addition to using our formal powers, we may also request that a controller or processor provides information to us voluntarily, either prior to, or during, an investigation. As set out in our Data Protection Fining Guidance, we may regard cooperation with us as a mitigating factor when we are considering imposing a fine and its amount.[30] This may include a controller or processor responding to requests during our investigation in a way that enables us to conclude the enforcement process significantly more quickly or effectively. This cooperation is in addition to a controller or processor's ordinary duty of cooperation that is required by law and therefore not a mitigating factor.[31] By contrast, we may view persistent and

[29] Raising concerns about our process during an investigation should be distinguished from the right to make a data protection complaint under section 165 DPA 2018. For more information about making a data protection complaint, see our guidance on What to expect from the ICO when making a data protection complaint | ICO.
[30] ICO, Data Protection Fining Guidance, March 2024, paragraph 88.
[31] See article 31 UK GDPR and section 63 DPA 2018.

repeated behaviour that delays regulatory action as an aggravating factor.[32]

4.1 Information notices

71. An information notice is a formal written request to provide us with information or documents to help us carry out our functions.

72. We may require a controller or processor to provide us with information or documents that we reasonably require to carry out our functions under data protection law.[33] We do not need to have opened an investigation in order to send information notices to controllers or processors. For example, we may give information notices to controllers or processors in the following circumstances:

    - as part of our function to monitor compliance with data protection legislation and relevant developments[34];
    - in the exercise of our power to carry out data protection audits[35];
    - to provide advice to Parliament or the government[36]; or
    - to give an opinion.[37]

73. If the controller or processor is not established in the UK, we may make the request to its representative designated under article 27 UK GDPR.[38]

74. We may also require any person to provide us with information or documents that we reasonably require to:

    - investigate certain suspected infringements of data protection legislation or a suspected criminal offence under the DPA 2018[39]; or
    - determine whether processing of personal data is carried out by someone in the course of a purely personal or household activity.[40]

75. An information notice:

    - explains the legal basis for sending it and why we require the information or documents we are requesting;
    - specifies or describes the information or documents, or both, that we

[32] ICO, Data Protection Fining Guidance, March 2024, paragraph 89.
[33] Section 142(1)(a) DPA 2018.
[34] Article 57(a) and (i) UK GDPR and paragraphs 1(1)(a) and (h), schedule 13 DPA 2018.
[35] Article 58(1)(b) UK GDPR and section 115(6) DPA 2018. See the ICO website for more details about our Audit work.
[36] Section 115(3)(a) DPA 2018.
[37] Section 115(3)(b) DPA 2018.
[38] Section 142(9) DPA 2018.
[39] Section 142(1)(b)(i) DPA 2018. The relevant failures are those of a type described in section 149(2) DPA 2018.
[40] Section 142(1)(b)(ii) DPA 2018.

require; and

- specifies the form the controller or processor need to provide the information or documents in and where and when they must do so.[41]

76. We also explain the consequences of failing to comply with the information notice and the rights the recipient has to appeal it.[42]

77. The information notice sets a deadline that we must receive the response by. When determining this timescale, we consider the:

- nature and amount of information or documents required;
- resources likely to be available to the recipient; and
- impact on the timeliness of our investigation or delivery of other regulatory actions.

78. We are required to give recipients of information notices at least 28 calendar days to provide us with the information we require.[43] However, we may give a longer timescale if the information we are asking for is:

- a large amount;
- complex; or
- likely to be difficult for the recipient of the notice to obtain.

79. We may require a recipient to provide some information or documents we request in an information notice more quickly than other information (although we cannot require it sooner than 28 calendar days). For example, information or documents that are likely to be readily available, such as general corporate information or a controller or processor's privacy and data protection policies. As set out in our Data Protection Fining Guidance, we may view cooperation that enables us to conclude the enforcement process significantly more quickly or effectively as a mitigating factor.[44]

80. In most circumstances, it is reasonable and appropriate to give an information notice to a recipient without engaging with them first. In particular in the following situations:

- It is a simple request or the request is for standard information or documents known to be held by the recipient. For example, general corporate information, turnover or other financial information, or a controller or processor's privacy and data protection policies (including data protection impact assessments, legitimate interest

[41] Section 142(3) DPA 2018.
[42] Section 142(4) DPA 2018.
[43] Section 142(5) DPA 2018 and rule 22(1) of The Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009.
[44] ICO, Data Protection Fining Guidance, paragraph 88.

assessments, transfer risk assessments, and records of processing activities).

- We are opening an investigation or exercising our enforcement powers in circumstances where we do not consider that giving prior notice about an information notice would be appropriate because we are concerned about the possibility of the controller or processor destroying information or documents.
- The controller or processor has already provided us with the information on a voluntary basis and we wish to ensure that it is complete and accurate.
- We are asking for updates to information previously provided, particularly if the questions are the same or very similar to the questions we previously asked.
- We are giving similar information notices to several controllers or processors at the same time which means that prior engagement is not practical.

81. Unless otherwise indicated, the controller or processor should send its response to us in electronic format. (See section 5.3 Handling confidential information for the process for providing representations about the confidential nature of information contained in the response).

82. We cannot require the recipient of an information notice to provide us with certain legally privileged information[45] (see section 5.1 Privileged communications) or certain information that would require a person to admit a criminal offence (see section 5.2 Privilege against self-incrimination).[46]

83. We can only require a controller or processor to provide information about processing personal data for the special purposes relating to journalism or academic, artistic or literary purposes if we have:

- made a determination under section 174 DPA 2018; or
- reasonable grounds to suspect that we could make such a determination and we need the information to make it.[47]

84. In some circumstances, we may require a controller or processor to provide information or documents urgently.[48] If so, the information notice will inform the recipient of the time when it must provide the information and explain the reasons for the urgency. We cannot require a recipient to

[45] Section 143(3) to (5) DPA 2018. We also cannot require a person to give us information to the extent that would involve an infringement of the privileges of either House of Parliament (section 143(2) DPA 2018).
[46] Section 143(6) to (8) DPA 2018.
[47] Section 143(1) DPA 2018. See Section 5.4 Determination relating to the special purposes.
[48] Section 142(7) DPA 2018.

provide information less than 24 hours after giving the information notice. If we require a recipient to provide information urgently, we are unlikely to engage with it first.

85. Circumstances in which we may consider it appropriate to require a controller or processor to provide information or documents urgently include, but are not limited to, where we need to:

- prevent or limit damage or distress to people;
- mitigate the impact of a personal data breach or a suspected infringement of data protection legislation;
- prevent the controller or processor destroying or disposing of information or documents; or
- meet a statutory deadline or other legal obligation that applies to us.

86. We also take into account the factors set out at paragraphs 77 and 78 when deciding whether to give an urgent information notice.

87. We expect recipients to comply fully with an information notice within the given deadline. If a recipient considers that it needs more time to respond to the information notice, it should raise this with us as soon as possible. In all circumstances, recipients must provide reasons for requesting an extension to the deadline we have set. We treat any requests on a case-by-case basis, considering the reasons given, while also taking into account minimising delays to our investigation or other regulatory action.

88. If a recipient does not comply with all of the requirements in an information notice, we may:

- give an assessment notice (see section 4.2 Assessment notices);
- give an interview notice (see section 4.3 Interview notices);
- apply to court for an information order requiring the recipient to provide us with information or documents referred to in the information notice or any other information or documents the court is satisfied we require[49]; or
- give a fine to the recipient for failing to comply with an information notice (see section 10 Process for giving penalty notices).[50]

89. We decide how to proceed by taking into account the relevant circumstances of failing to comply, including:

[49] Section 145 DPA 2018. The jurisdiction of the courts for this purpose is set out in section 180 DPA 2018.
[50] Section 155(1)(b) DPA 2018. See also the ICO's Data Protection Fining Guidance, in particular paragraphs 61 and 68.

- the reasons for the non-compliance;
- the extent of the non-compliance; and
- its impact on our ability to progress our investigation or discharge our functions.

90. We also take into account the need to ensure there is an effective deterrent against recipients not complying with information notices. This may mean we take immediate steps to obtain the information we need (eg by giving an assessment notice to permit us to enter specified premises, giving an interview notice, or applying to the court for an information order). We may also impose a fine for failing to comply.

91. The recipient of an information notice must provide adequate and accurate information in its response. Failure to do so without reasonable excuse may lead to us taking enforcement action and imposing a fine. Furthermore, it is a criminal offence to:

- knowingly or recklessly make a statement in response to an information notice that is false in a material respect[51]; or
- intentionally prevent us from viewing or being provided with any information or document within the scope of an information notice by destroying, disposing of, concealing, blocking, or falsifying it.[52]

92. Therefore, a recipient of an information notice should carefully check the completeness and accuracy of the information it provides in its response before submitting it to us. It must also make sure it has provided a response to every question and in the format we requested. In particular, we may require a recipient to provide written information or documents in specified formats. For example, we may ask it to provide written information in a document (.docx) format or numerical information in a spreadsheet (.csv or .xlsx) format.

93. A recipient of an information notice may appeal to the Tribunal.[53] If it brings an appeal, a recipient does not need to provide the information requested in the notice pending the determination or withdrawal of the appeal, unless we have requested the information urgently.[54] A recipient of an urgent information notice may apply to the court to disapply the urgency statement or to change the time period that it is required to comply with the notice within.[55]

[51] Section 144 DPA 2018.
[52] Section 148 DPA 2018.
[53] Section 162 DPA 2018. For more information about the appeals procedure see The Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules.
[54] Section 142(6) and (7) DPA 2018.
[55] Section 164 DPA 2018.

94. We can cancel an information notice at any time by providing written confirmation of this decision to the recipient.[56]

95. We do not typically make a public announcement that we have given an information notice. However, there may be circumstances in which we consider it appropriate to do so (eg if we consider it is in the public interest or if we are providing updates on the progress of our work).

4.2 Assessment notices

96. An assessment notice is a formal written notice requiring a controller or processor to permit us to carry out an assessment of whether it has complied, or is complying, with data protection legislation.[57] This is an investigative power that allows us to enter specified premises and inspect documents, information, equipment and other material. It also allows us to require the preparation of reports by approved persons.

97. We have broad discretion to use assessment notices across the range of our functions under data protection legislation.[58] Therefore, we do not need to have opened an investigation in order to give an assessment notice to a controller or processor. For example, we may use an assessment notice in the exercise of our power to:

- carry out data protection audits as part of our audit work;[59]
- provide advice to Parliament or the government;[60] or
- give an opinion.[61]

98. We cannot give a controller or processor an assessment notice about processing personal data for the special purposes.[62]

99. We recognise that requiring a controller or processor to allow us to enter its premises to conduct an assessment is a significant step. Therefore, we exercise our discretion to give assessment notices and decide what actions we require a controller or processor to take in a way that is appropriate and proportionate, taking into account all relevant circumstances.

100. An assessment notice may require a controller or processor to take one or more of a range of actions to assist us.[63] These are to:

---

[56] Section 142(8) DPA 2018.
[57] Section 146(1) DPA 2018.
[58] See Leave.EU and Eldon Insurance v Information Commissioner [2021] UKUT 26 (AAC), paragraph 112.
[59] Article 58(1)(b) UK GDPR and section 115(6) DPA 2018. See the ICO website for more details about our Audit work.
[60] Section 115(3)(a) DPA 2018.
[61] Section 115(3)(b) DPA 2018.
[62] Section 147(5) DPA 2018. See Section 5.4 Determination relating to the special purposes.
[63] Section 146(2) DPA 2018. References to the Commissioner in section 146(2) include references to the Commissioner's officers and staff (see section 146(3) DPA 2018).

- permit us to enter specified premises;
- direct us to specified documents on the premises;
- assist us to view specified information that we are able to view using equipment on the premises;
- comply with a request from us for a copy (in a form that we may request) of:
    - the documents the controller or processor directs us to; and
    - the information the controller or processor assists us to view.
- direct us to specified equipment or other material on the premises;
- permit us to inspect or examine the documents, information, equipment or material;
- provide us with an explanation of such documents, information, equipment or material;
- permit us to observe the processing of personal data that takes place on the premises;
- make available a specified number of people of a specified description for us to interview who process personal data on behalf of the controller and who are willing to be interviewed;
- make arrangements for an approved person to prepare a report and provide it to us.[64]

101. In the assessment notice, we explain which of these actions the controller or processor is required to take. The assessment notice also provides information about the consequences of failing to comply with it (see paragraph 108) and the rights to appeal the notice.[65]

102. If we give an assessment notice to a processor we will, so far as reasonably practical, give a copy of the notice to each controller that the processor processes personal data for.[66]

103. We cannot require the recipient of an assessment notice to provide us with certain legally privileged information if it is connected to legal advice or proceedings relating to data protection legislation (see section 5.1 Privileged communications).[67] Therefore, we do not examine or inspect this

[64] The number of people made available for interview may not exceed the number who are willing to be interviewed. See section 146(2)(i) DPA 2018.
[65] Section 146(5) DPA 2018.
[66] Section 146(11) DPA 2018.
[67] Section 147(2) to (4) DPA 2018. We also cannot require a person to do something to the extent that requiring the person to do it would involve an infringement of the privileges of either House of Parliament (section 147(1) DPA 2018).

legally privileged information or documents containing this information. However, as explained in section 5.1, there is some legally privileged information we may examine and inspect when carrying out an assessment. If there is a dispute about whether we have the power to inspect or examine information or documents because of legal privilege, we will consider arranging for a lawyer who is independent of the ICO to review the material.

104. We are aware that when carrying out an assessment we may need to inspect and examine personal data (including special category information and criminal offence information) or confidential information that may be commercially sensitive. Depending on the circumstances, there may also be occasions when we need to view documents about a person's health or the provision of social care. If so, we seek to minimise the amount of this information we examine or take copies of. We keep this to what we need to assess whether the controller or processor has complied, or is complying, with data protection legislation. We are subject to strict rules governing the extent to which we are able to disclose confidential information (see section 5.3 Handling confidential information).

105. If the controller or processor is likely to have access to official, secret or top secret information, we ensure that the ICO staff present at the assessment include those with appropriate national security vetting.[68] We expect controllers or processors that receive an assessment notice to inform us as soon as reasonably possible after receiving the notice whether any of the requirements in the notice are likely to involve us inspecting or examining official, secret or top secret information.

106. The outcome of an assessment under an assessment notice depends on the function we are exercising. Where we give an assessment notice in the context of an investigation, we use the information we obtain to inform that investigation and help us decide whether to take any enforcement action. Information we have gathered during the assessment is included, as relevant, in any notice of intent, preliminary enforcement notice, warning, reprimand, enforcement notice or penalty notice.

107. If we give an assessment notice as part of our audit work, the information we obtain may form part of an audit report setting out our findings. We provide the audit report to the controller or processor and we typically publish an executive summary of the audit report on our website.[69] If we give an assessment notice in the context of one of our other functions, we may include information we obtain during the assessment, as relevant, in the publication of the outcome of that work. For example, as part of advice

[68] Information about security vetting is available here: United Kingdom Security Vetting. The ICO cannot give an assessment notice to a body specified in section 23(3) Freedom of Information Act 2000 (see section 147(6)(a) DPA 2018). These are bodies dealing with security matters, such as the Security Service, GCHQ and the National Crime Agency.
[69] See: Audits | ICO.

to Parliament or government, or if we give an opinion. In each case, we take into account the confidentiality of the information.

108. If a recipient does not comply with a requirement in an assessment notice, we may:

- apply to court for a warrant[70]; or
- take enforcement action by imposing a fine on the recipient for failing to comply with an assessment notice (see section 10 Process for giving penalty notices).[71]

109. We decide how to proceed by taking into account the relevant circumstances of the failure to comply. This includes the reasons for the non-compliance, the extent of the non-compliance, and its impact on our ability to progress our investigation or discharge our functions. We also take into account the need to ensure an effective deterrent against controllers or processors not complying with assessment notices. This may mean that we take immediate steps to obtain the information we need by applying to court for a warrant to permit us to enter specified premises and obtain the information.[72] We may also impose a fine for failing to comply with the assessment notice and take other steps to obtain the information we need, such as giving an interview notice (see section 4.3 Interview notices).

110. A recipient of an assessment notice must ensure that it fulfils the requirements set out in the notice. It is a criminal offence to intentionally prevent us from viewing, being provided with or directed to any information, document, equipment or material required by an assessment notice by (as relevant) destroying, disposing of, concealing, blocking, or falsifying it.[73]

111. A recipient of an assessment notice may appeal to the Tribunal.[74] If an appeal is brought, the controller or processor does not need to comply with the requirements in the notice pending the determination or withdrawal of the appeal, unless we have requested the information urgently.[75] A recipients of an urgent assessment notice may apply to the court to disapply the urgency statement or to change the time period that it is compelled to comply to the notice within.[76]

[70] Section 154 and paragraph 2, schedule 15 DPA 2018 (Issue of warrants in connection with assessment notices). See Section 4.4 Powers of entry and inspection.
[71] Section 155(1)(b) DPA 2018. See also the ICO's Data Protection Fining Guidance, in particular paragraphs 61 and 68.
[72] See paragraph 5(3), schedule 15 DPA 2018.
[73] Section 148 DPA 2018.
[74] Section 162 DPA 2018. For more information about the appeals procedure see The Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules.
[75] Section 146(7) DPA 2018.
[76] Section 164 DPA 2018.

112. We do not typically make a public announcement that we have given an assessment notice. However, there may be circumstances in which we consider it appropriate to do so (eg if we consider it is in the public interest or if we are providing updates on the progress of our work).

4.2.1 Factors we consider when deciding to give an assessment notice

113. When deciding whether to give an assessment notice to a controller or processor, we consider a range of factors. We are more likely to give an assessment notice in the following circumstances:

- If we are unlikely to obtain the evidence we need using an information notice (eg because we consider it is reasonably necessary to examine equipment or observe the processing of personal data on the premises). This is more likely to be the case if the processing operations are complex or the information we require relates to the implementation of technical and organisational measures.
- If the controller or processor has refused to voluntarily provide the information we need or allow us to enter its premises. Unless we need to act urgently or we suspect there is a serious failing, we typically ask a controller or processor if it is willing to cooperate to provide the information we need or to allow us access to its premises, before giving an assessment notice.
- If the controller or processor has failed to fully comply with an information notice, either relating to the same subject matter or about another matter in the past.
- If we suspect there is a serious failure to comply with data protection legislation, particularly if that failure appears to be ongoing or if we have previously given the controller or processor with a warning about its intended processing. In these circumstances, we may require the controller or processor to comply with some, or all, of the requirements in the assessment notice urgently (see section 4.2.2 Specifying the time for compliance and urgent assessment notices).
- If we need to obtain evidence about compliance with an enforcement notice. We are more likely to give an assessment notice if we have concerns that the controller or processor has failed, or is failing to, comply with a requirement in an enforcement notice. For example, this may be because we have received complaints about such a failure to comply.
- If we are assessing similar processing by multiple controllers or processors and we want to be consistent in our approach.

4.2.2 Specifying the time for compliance and urgent assessment notices

114. For each requirement in an assessment notice, we specify the time or the period that the controller or processor must comply within.[77]

115. We are generally required to give the controller or processor at least 28 calendar days to comply with any requirements in an assessment notice.[78]

116. Where possible, we aim to provide controllers or processors with a copy of the assessment notice in draft form before we formally give it to them. This ensures that the assessment notice is appropriately targeted and sufficiently clear to enable the recipient to meet the requirements within the proposed timeframe.

117. If we give an assessment notice in draft form, we allow a reasonable period of time for the controller or processor to comment on the proposed requirements set out in the draft notice. In particular, this includes comments about the proposed date for complying with the requirement to permit us to enter specified premises and the availability of people we require it to make available for interview, and, if relevant, the time period proposed for providing a report by an approved person.

118. We take into account any comments on the draft assessment notice and decide whether we consider it appropriate to amend the final assessment notice before giving it to the controller or processor.

119. In some cases, we may require a controller or processor to comply with a requirement in an assessment notice urgently. If that is the case, the assessment notice informs the recipient of the time they must comply with the requirement by and explains the reasons for the urgency. In urgent cases, we do not provide a copy of a draft assessment notice in advance, unless we consider there is a compelling reason to do so.

120. We may require a controller or processor to comply with an assessment notice in less than seven days if:

- we have reasonable grounds to suspect a controller or processor has failed, or is failing, to comply with data protection legislation or that an offence under the DPA 2018 has been, or is being, committed[79];

[77] Section 146(4) DPA 2018.
[78] Section 146(6) DPA 2018 and rule 22(1) of The Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009.
[79] Section 146(9)(a) DPA 2018. The relevant failures are those of a type described in section 149(2) DPA 2018. Offences under the DPA 2018 include destroying or falsifying information and documents (section 148 DPA 2018), the unlawful obtaining or disclosing personal data (section 170 DPA 2018), and the unlawful re-identification of de-identified personal data (section 171 DPA 2018).

- the assessment notice does not specify domestic premises[80]; and
- we consider it necessary for the recipient to comply with a requirement in less than seven days.[81]

121. If we do not have reasonable grounds to suspect a failure or offence, or the assessment notice specifies domestic premises, the minimum period we can require for compliance with an urgent requirement is seven days.

122. The assessment notice explains the reasons for the urgency and, where relevant, indicates the nature of the suspected failure or offence.[82]

123. The circumstances where we consider it appropriate to require a controller or processor to comply with an assessment notice urgently include if it is reasonably necessary to:

- prevent or limit damage or distress to people;
- mitigate the impact of a personal data breach or a suspected infringement of data protection legislation, particularly if we have concerns the suspected infringement is likely to be serious;
- prevent the destruction or disposal of information, documents, equipment or material;
- assess compliance with a requirement in an enforcement notice where we suspect there is a failure to comply; or
- meet a statutory deadline or other legal obligation that applies to us.

4.2.3 The nature of inspections and examinations carried out under an assessment notice

124. In carrying out inspections and examinations under an assessment notice, we follow the requirements in the DPA 2018 and take into account the Home Office's code of practice on powers of entry,[83] where relevant.

125. We exercise our power of entry under an assessment notice at a reasonable hour. We determine what constitutes a 'reasonable hour' based on the normal working practices of the controller or processor.[84]

126. When we arrive at the premises, the person authorised to lead the assessment shows the occupier the following, if asked to do so:

- evidence of their identity;

[80] Section 146(9)(c) DPA 2018.
[81] Section 146(9)(d) DPA 2018.
[82] Section 146(8)(b), (9)(b) and (9)(e) DPA 2018.
[83] Home Office, Powers of Entry: code of practice, December 2014.
[84] Home Office, Powers of Entry: code of practice, December 2014, paragraph 13.1.

- the assessment notice; and
- their authorisation to exercise the power of entry and inspection.

127. More than one person may be authorised to attend the premises. The number of people present reflects what we consider is reasonable and proportionate in the circumstances.[85]

128. The controller or processor may have legal advisers present at the premises throughout our assessment. If we have given seven or more calendar days' notice of our intention to carry out the assessment, we expect that any legal advisers who plan to attend will be present on our arrival. We will not wait for them to arrive before commencing our entry and inspection. If we have not given the controller or processor notice of the assessment and there is no in-house legal adviser on the premises, we may wait a reasonable time for a legal adviser to arrive.

129. The nature of the inspections and examinations during an assessment depend on the individual circumstances of the case and the requirements set out in the assessment notice.[86] We can also require a controller or processor to make copies of any documents it directs us to or information it assists us to view.[87]

130. During that assessment, we expect controllers or processors to give reasonable assistance to us.[88] This assistance may include for example opening locked doors or containers, or providing passwords to access password-protected information.

4.2.4 The nature of interviews carried out under an assessment notice

131. We may require a controller or processor to make any number of people of a specified description who process personal data on behalf of the controller available for interview.[89] The people it makes available for interview must be willing to be interviewed. We cannot compel people to be interviewed or answer questions using our assessment notice power. We can only require people to answer questions using an interview notice (see section 4.3 Interview notices).

132. We conduct interviews during an assessment to enable us to understand how the controller or processor processes personal data and to assess whether it has complied, or is complying, with data protection legislation.

[85] Home Office, Powers of Entry: code of practice, December 2014, paragraph 9.1.
[86] Section 146(2) DPA 2018.
[87] Section 146(2)(d) DPA 2018.
[88] Home Office, Powers of Entry: code of practice, December 2014, paragraph 18.1. See also the requirement in article 31 UK GDPR for controllers and processors and, where applicable, their representatives to cooperate on request with the Commissioner. See also section 63 DPA 2018.
[89] Section 146(2)(i) DPA 2018.

133. Where possible, we agree who we would like to interview in advance of the assessment and arrange a schedule for the interviews. It is the controller or processor's responsibility to inform these people that they are to be interviewed and to give them adequate time to prepare. We endeavour to provide in advance a list of topics that we would like to discuss with them. These are likely to include questions about:

    - what personal data is processed;
    - how it is processed (including technical and operational measures that the controller or processor has in place); and
    - the purpose of any such processing.

134. We may conduct interviews at a person's desk or in a separate room, depending on the circumstances and the environment. We may also agree to conduct interviews virtually, taking into account someone's geographical location, their working pattern, and the cost and time required for them to attend in person. We also consider any other reasonable adjustments that we need to make.

135. We typically interview people individually. However, we may agree to interview people together if we consider that is appropriate and will not prejudice our assessment. Given the voluntary nature of the interviews, we do not consider it necessary for interviewees to be accompanied by a legal adviser or a representative of the controller or processor that receives the assessment notice. However, if someone asks to be accompanied, we will not object to this, provided it does not unreasonably delay the assessment. Therefore, we expect any requests to be made at the time we arrange the interview schedule.

136. In some circumstances, in particular if we are carrying out an urgent assessment, we may not be able to identify everyone we require the controller or processor to make available for interview in advance. If so, we seek to arrange interviews during the assessment or agree that the interviews take place at a later date. Our power to require people to be made available for interview is separate from our power to require the controller or processor to provide us with an explanation of documents, information or equipment.[90]

137. We either record the interview or take a note at the time of the questions we ask and the interviewee's responses. After the assessment, we provide a copy of the recording, any transcript of the recording or our note of the interview and ask the interviewee to confirm, in writing, that it is an accurate account.

[90] Section 146(2)(g) DPA 2018.

4.2.5 Reports of approved persons

138. We may include a requirement in an assessment notice for a controller or processor to arrange for an approved person[91] to prepare a report on a specified matter and provide it to us.[92]

139. If so, we may require the arrangements to include specified terms about:

- how they should prepare the report;
- what they should include in the report;
- what form they should provide the report in; and
- the date they should complete the report by.[93]

140. The controller or processor must nominate someone to prepare the report within a period specified in the assessment notice.[94] The controller or processor should explain why they consider the nominated person is suitable.

141. If we are satisfied that the nominated person is suitable, we send a written notice to the controller or processor to approve them.[95]

142. If we are not satisfied that the nominated person is suitable, we send a written notice to the controller or processor to:

- inform the controller or processor that we have decided not to approve the nominated person to prepare the report;
- inform the controller or processor of the reasons for our decision; and
- approve a person who we are satisfied is suitable to prepare the report.[96]

143. If the controller or processor does not nominate a person within the period specified in the assessment notice, we approve someone who we are satisfied is suitable and inform the organisation by written notice.[97]

[91] An "approved person", in relation to a report, means a person approved to prepare the report in accordance with section 146A DPA 2018 (section 146(11) DPA 2018).
[92] Section 146(2)(j) and (k) DPA 2018.
[93] Section 146(3A) DPA 2018.
[94] Section 146A(2) DPA 2018.
[95] Section 146A(3) DPA 2018.
[96] Section 146A(4) DPA 2018.
[97] Section 146A(5) DPA 2018.

144. The controller or processor is liable for paying the approved person's remuneration and expenses under the arrangements.[98]

145. We will decide on a case-by-case basis the specific requirements for the preparation of an approved person report, including the type and frequency of communication between us and the approved person. Typically, we will request the opportunity to review the proposed terms of appointment and to comment on any draft reports before receiving the final report.

Factors we consider when deciding whether to give an assessment notice that imposes a requirement for an approved person to prepare a report

146. When deciding whether to give an assessment notice that imposes a requirement for an approved person to prepare a report, we consider the following factors, as relevant:

- whether a report would assist us in identifying, understanding or assessing a specified matter including, for example:
    - understanding the nature and extent of the processing of personal data which we suspect may not comply with data protection legislation; or
    - assessing the security measures taken to protect personal data;

- whether the controller or processor is able and willing to provide the information we require, or whether they are unlikely to provide it through:
    - a lack of cooperation;
    - a lack of appropriate skills or resources; or
    - issues resulting from poor record-keeping and management information systems;

- whether the controller or processor under investigation has given us all the relevant information or has not obtained sufficiently detailed information about a suspected infringement of data protection legislation;

- whether the controller or processor has an existing report which it has not provided to us in full or in part, or has provided an existing report which is limited or inadequate, or we would otherwise benefit from an independent report (eg because it is necessary for an independent third party to verify particular data);

- whether the matter is sufficiently technically complex that it requires specialist skills or resources that we do not have available at the required time;

[98] Section 146(11A) DPA 2018.

- whether using our other powers is more appropriate;
- whether a report would assist us in assessing compliance with data protection legislation, or monitoring any measures a controller or processor has taken to achieve compliance;
- whether a report would assist us in assessing, monitoring or understanding any risk of failure to comply with data protection legislation and how to prevent, limit or reduce that risk; or
- the potential costs of producing a report and their impact on the controller or processor as compared to the report's potential benefits.

147. The assessment notice typically gives the controller or processor 28 days to nominate someone to prepare the report. However, in some cases, we may require a controller or processor to comply with a requirement for an approved person to prepare a report more urgently (see paragraphs 119-123 above).

148. We will assess the suitability of the nominated person, taking into account the factors set out below (Factors we consider in determining the suitability of an approved person to prepare a report). If we approve the nominated person, we will inform the controller or processor in writing. If we do not approve the nominated person we will explain our reasons for not approving them and will, at the same time, notify the controller or processor of the person we have approved to prepare a report. If the controller or processor fails to nominate a person within the deadline for the nomination, we notify the controller or processor of the person we have approved to prepare a report.

Factors we consider in determining the suitability of an approved person to prepare a report

149. In determining the suitability of an approved person, we may take into account the following factors:

- whether they have the skills, expertise, experience and relevant qualifications required to address the matters specified in the assessment notice;
- whether there are any conflicts of interest or any other circumstances that may affect their ability to provide an independent, impartial and objective report;
- the availability of the approved person to give sufficient time to producing the report in the required timeframe; and

- the costs associated with producing the report.

150. In order to assess the costs associated with producing the report, we request the controller or processor provides us with details of estimates that the controller or processor has obtained from the nominated approved person and, where relevant, any other persons it has considered may be suitable to prepare the report (including any supplementary fees, eg VAT or administrative expenses). Where we do not approve the person nominated by the controller or processor, we will obtain cost estimates ourselves before approving a person we consider is a suitable person to prepare the report.

151. When we take into account the costs of producing the report, we consider the following factors:

- whether the controller or processor may gain some benefit from the work carried out by the approved person (eg a better understanding of the operation of, or improvements to, its systems);

- whether the work to be carried out by the approved person is work that should reasonably have been carried out by the controller or processor on its own initiative (eg a compliance review of a new system);

- whether the requirement for a report is due wholly, or in part, to the controller or processor's poor record keeping or management information systems such that the required information is not readily available or the analysis of the required information cannot readily be performed without the assistance of an approved person;

- whether the controller or processor under investigation has given us all the relevant information or has not obtained sufficiently detailed information about a suspected infringement of data protection legislation;

- whether the controller or processor has an existing report which it has not provided to us in full or in part, or it has provided an existing report which is limited or inadequate;

- the seriousness of possible infringements of data protection law and the possible need for further action; or

- the level of cooperation by the controller or processor and any relevant steps it's taken to prevent or mitigate the effects of any infringement of data protection law.

152. The controller or processor is liable for paying the approved person's remuneration and expenses for preparing the report.[99]

153. It is the duty of the controller or processor to give the approved person all the assistance they may reasonably require to prepare the report.[100] If we are satisfied that a controller or processor has failed to comply with that duty, we may give them a fine (see section 10 Process for giving penalty notices).[101]

154. Once we have approved the person, they should prepare the report in line with the requirements set out in the assessment notice.

4.3 Interview notices

155. An interview notice is a formal written request to an individual to attend at a place specified in the notice, and answer questions about any matter relevant to the investigation.[102]

156. We can only give an interview notice if we suspect that a controller or processor has failed, or is failing, to comply with data protection legislation, or has committed, or is committing, an offence under the DPA 2018.[103]

157. In addition, we can only give an interview notice to investigate the suspected failure or offence to an individual that is:

- the controller or processor;
- employed by, or otherwise working for, the controller or processor (or was at any time); or
- involved in the management or control of the controller of processor (or was at any time).[104]

158. An interview notice:

- specifies the time the individual must attend at the specified place and answer questions;[105]
- indicates the nature of the suspected failure or offence that is the subject of the investigation;
- provides information about the consequences of failing to comply

[99] Section 146(11A) DPA 2018.
[100] Section 146A(6) DPA 2018.
[101] Section 155(1)(c) DPA 2018.
[102] Section 148A(2) DPA 2018.
[103] Section 148A(1) DPA 2018. The relevant failures are those of a type described in section 149(2) DPA 2018. Offences under the DPA 2018 include destroying or falsifying information and documents (section 148 DPA 2018), the unlawful obtaining or disclosing personal data (section 170 DPA 2018), and the unlawful re-identification of de-identified personal data (section 171 DPA 2018).
[104] Section 148A(3) DPA 2018.
[105] Section 148A(4) DPA 2018.

with the notice; and

- provides information about the rights of the recipient to appeal it.[106]

159. We may cancel or vary an interview notice at any time by providing written notice to the recipient.[107]

4.4.1 Factors we consider when deciding whether to give an interview notice

160. We consider a range of factors when deciding whether to give an interview notice to an individual and are more likely to give an interview notice where:

- it helps us to understand how personal data is or was being processed, particularly where the processing is complex;
- it allows us to gather information more quickly and efficiently;
- it is useful to obtain first-hand accounts about the circumstances, particularly if the facts are unclear or disputed;
- we have previously asked to interview someone voluntarily but our request was refused; or
- there are difficulties in gathering the information we need by other means, such as information notices or assessment notices (eg because there is no or limited recorded information or the processing is covert).

4.4.2 Specifying the time for compliance and urgent interview notices

161. We cannot require someone to attend at the specified place and answer questions before the end of the period within which a recipient of an interview notice can appeal.[108] They can appeal within 28 days of the date on which we send the notice.[109] If a recipient appeals, they do not need to attend at the specified place and answer questions until the determination or withdrawal of the appeal,[110] unless we have requested the interview urgently.[111]

162. We may require someone to attend at the specified place and answer questions urgently (eg before the end of the period within which the recipient can appeal).[112] If so, the interview notice informs the individual of

[106] Section 148A(5) DPA 2018.
[107] Section 148(9) DPA 2018.
[108] Section 148A(6) DPA 2018.
[109] Rule 22(1) of The Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009.
[110] Section 148A(7) DPA 2018.
[111] Section 142(6) and (7) DPA 2018.
[112] Section 148A(8) DPA 2018.

the time when they must attend at the specified place and explain the reasons for the urgency. We cannot require a recipient to attend an interview less than 24 hours after giving the interview notice.[113] Where possible, we try to give seven days' notice of an urgent interview.

163. Circumstances in which we may consider it appropriate to require someone to attend an interview and answer questions urgently include, but are not limited to, where:

- it is necessary to ensure that personal data is protected or to prevent or limit damage or distress;
- it will mitigate the impact of a personal data breach or suspected infringement;
- there is a risk that the individual person may not be available to attend in person at a later date; or
- we need the information urgently because of a statutory deadline (eg to give a penalty notice).

164. A recipient of an urgent interview notice may apply to the court to disapply the urgency statement or to change the time period that they are required to comply with the notice.[114]

4.4.3 Nature of interviews carried out under an interview notice

165. Typically, we hold interviews at one of our offices. However, we may decide that it is appropriate to conduct the interview elsewhere at another location or virtually. We take into account all relevant factors in making this decision, including the individual's location and the cost and time involved for them to attend in person. We do not reimburse any costs incurred by the individual to attend the interview (eg travel costs or the cost of legal advice).

166. We will conduct interviews in accordance with any relevant and applicable national guidelines. Prior to the interview, we may provide the individual with a list of topics or other information. In particular, where we intend to seek explanations of documents during the interview, we provide these in advance. However, in some cases, it may not be possible or appropriate for us to provide information or documents in advance. We will not provide a list of questions in advance of the interview.

167. The individual may only be accompanied by their own legal adviser at the interview. This should not be a legal adviser who is also acting for the controller or processor (where that is not the individual). Our interview notice power requires the individual to answer questions. Therefore, it is

[113] Section 148A(8)(b) DPA 2018.
[114] Section 164 DPA 2018.

not the legal adviser's role to answer questions on an individual's behalf. If we consider that the interview is being obstructed by the conduct of the legal adviser, we may treat that as a failure to cooperate with our investigation and, if necessary, take steps if we consider that the individual is not complying with the interview notice.

168. Typically, we record interviews, but in circumstances where this is impracticable, we take a note at the time of the questions we ask and the interviewee's responses. After the interview, we provide a copy of any transcript of the recording or our note of the interview and ask the interviewee to confirm, in writing, that it is an accurate account.

169. If an individual needs to vary the place or time specified in the interview notice, or requires translation services or any reasonable adjustments due to a disability, they should request this variation or requirement as soon as possible. We treat any requests on a case-by-case basis. We consider the reasons given, while also taking into account the importance of minimising delays to our investigation or other regulatory action.

170. An individual is required to comply with an interview notice and attend at the place specified in the notice and answer questions about any matter relevant to the investigation,[115] subject to the following restrictions:

- We cannot require someone to answer questions about certain legally privileged communications[116] (see section 5.1 Privileged communications).
- We cannot require someone to answer questions if doing so would, by revealing the evidence of commission of an offence, expose the individual to proceedings for that offence (see section 5.2 Privilege against self-incrimination).[117]
- We cannot give an interview notice about processing of personal data for the special purposes.[118]
- We cannot give an interview notice to an individual for the purpose of investigating a suspected failure or offence if the controller or processor suspected of the failure or offence is a body specified in section 23(3) of the Freedom of Information Act 2000 (bodies dealing with security matters).[119]

[115] Section 148A(2) DPA 2018.
[116] Section 148B(2) to (4) DPA 2018. We also cannot require an individual to answer questions to the extent that requiring the person to do so would involve an infringement of the privileges of either House of Parliament (section 148B(1) DPA 2018).
[117] Section 148B(5) to (7) DPA 2018.
[118] Section 148B(8) DPA 2018.
[119] Section 148B(9) DPA 2018.

171. If a recipient fails to comply with an interview notice, we may give a fine to that individual (see section 10 Process for giving penalty notices).[120] This reflects the fact that a failure to cooperate can prevent us from fully understanding the facts of the case or progressing our investigation in a timely way. We decide how to proceed by taking into account the relevant circumstances of the failure to comply, including:

    - the reasons for the non-compliance;
    - the extent of the non-compliance; and
    - its impact on our ability to progress our investigation or discharge our functions.

172. It is an offence for an individual, in response to an interview notice, to make a statement which the individual knows to be false in a material respect, or recklessly to make a statement which is false in a material respect.[121]

173. We do not typically make a public announcement that we have given an interview notice. However, there may be circumstances when we consider it appropriate to do so (eg if we consider it is in the public interest or if we are providing updates on the progress of our work).

[120] Section 155(1)(b) DPA 2018. See also the ICO's Data Protection Fining Guidance, in particular paragraphs 61 and 68.
[121] Section 148C DPA 2018.

4.4 Powers of entry and inspection

174. We may apply for a warrant to enter and inspect specified premises where a controller or processor has failed to comply with an assessment notice.[122]

175. In addition, we may apply for a warrant if:

- there are reasonable grounds for suspecting that a controller or processor has failed, or is failing, to comply with data protection legislation, as described in section 149(2) DPA 2018 or an offence under the DPA 2018 has been committed; and
- there are reasonable grounds to suspect that we will find evidence of the failure to comply or the commission of the offence on the premises specified or we will be able to view it using equipment on these premises.[123]

176. In order to obtain a warrant we must satisfy a judge of the High Court, a circuit judge or a District Judge (Magistrates' Court) by information on oath supplied by the Commissioner that these conditions are met.[124]

177. Schedule 15 DPA 2018 sets out a range of requirements about issuing warrants.

5 Limits on our powers of investigation

178. As a public body, we act fairly and reasonably when enforcing data protection legislation and using our statutory powers. We also act in accordance with the statutory limits on our powers of investigation set out in the DPA 2018.

179. We explain below the areas where the DPA 2018 imposes limits on the information we can obtain and how we use it. These are:

- privileged communications;
- privilege against self-incrimination;
- handling confidential information; and
- determinations relating to the special purposes.

[122] Paragraph 2, schedule 15 DPA 2018.
[123] Paragraph 1, schedule 15 DPA 2018.
[124] Paragraphs 1(1) and 2(1), schedule 15 DPA 2018. See also paragraphs 18 and 19, schedule 15 DPA 2018 in relation to applications for warrants in Scotland and Northern Ireland, respectively.

5.1 Privileged communications

180. We are required to publish guidance about how we:

- ensure that any privileged communications[125] we obtain or have access to in the course of our functions are only used or disclosed so far as is necessary to carry out those functions; and
- comply with restrictions and prohibitions on obtaining or having access to privileged communications imposed by legislation.[126]

181. We do not use our powers of investigation to require anyone to produce or disclose privileged communications to us unless we consider it is necessary for us to perform our functions. This is only likely to be the case in limited circumstances and our ability to do so is circumscribed by the DPA 2018.

182. We are only allowed to require a person to give or disclose privileged communications to us, answer questions about privileged communications, or exercise our powers of inspection and seizure under warrant about privileged communications to the extent that the communications do not relate to communications between:

- a professional legal adviser and the adviser's client in connection with the giving of legal advice to their client with respect to obligations, liabilities or rights under data protection legislation; or
- a professional legal adviser and the adviser's client (or between such an adviser or client and another person) in connection with, or in contemplation of, proceedings under or arising out of data protection legislation, for the purposes of such proceedings.[127]

183. In other words, we cannot compel a person to produce or disclose or answer questions about communications protected by legal advice or litigation privilege connected to data protection legislation. However, we may compel a person to produce or disclose or answer questions about other types of privileged communications which contain information that we reasonably require (eg legal advice about another area of law).

184. We recognise that the abrogation of legal professional privilege by statute in this way is not commonplace and that the protection of privileged communications is a fundamental right. However, as contemplated by Parliament in passing the DPA 2018, these provisions are necessary to ensure that we retain the power to investigate potential infringements of

[125] Section 133(5) DPA 2018 defines "privileged communications" in line with the common law concepts of legal advice privilege and litigation privilege.
[126] Section 133(1) DPA 2018. Section 133(1)(b) refers to restrictions or prohibitions imposed by "an enactment". "Enactment" is defined in section 205(1) DPA 2018.
[127] See section 143(3) to (5) DPA 2018 in relation to information notices, section 147(2) to (4) DPA 2018 in relation to assessment notices, and paragraph 11, schedule 15 DPA 2018 in relation to our powers of entry and inspection.

data protection legislation by professional legal advisers, such as law firms.[128] Therefore, we only use our powers to obtain privileged communications if we have reasonable grounds to suspect that we require the information contained within them to carry out our functions under data protection legislation.

185. If there is a dispute about whether communications, or part of communications, are privileged because of their connection to data protection legislation and therefore not disclosable, we will consider arranging for a lawyer who is independent of the ICO to review the material. If we decide this is necessary to maintain the proper protections of privileged communications, we will take into account the Bar Council's guidance on Legal Professional Privilege – Independent Counsel in relation to seized material.[129]

186. If such a dispute arises during an inspection of premises by us, either under an assessment notice or warrant, the authorised ICO staff member present may request that the communications are placed in a sealed envelope or package. We will then discuss the arrangements for the safe keeping of these items by us pending resolution of the dispute. This includes ensuring that the disputed communications are isolated and stored securely. If we are exercising our power to inspect or seize documents under warrant, we also take into account the provisions about legal professional privilege in the Attorney General's Guidelines on disclosure.[130]

187. If we obtain privileged communications in the exercise of our functions, we store them securely and limit access appropriately. We only use this material to the extent necessary for carrying out our functions and only disclose it if we have lawful authority. We take into account the significant public interest in protecting the confidentiality of legal advice and communications for the purpose of litigation.[131]

188. A person may wish to waive privilege in legally privileged material we request or wish to provide it to us for their own purposes. This is a matter of choice for them. However, should they choose to do so, we do not accept any condition to a waiver of privilege that restricts or fetters our ability to use that material to exercise our statutory functions.

5.2 Privilege against self-incrimination

189. When we require a controller or processor or any other person to provide information to us using an information notice, we cannot force them to do so if it would, by revealing evidence of an offence, expose the person to

[128] See, for example, Hansard HL Deb. vol. 787 cols. 31 to 35, 20 November 2017.
[129] The Bar Council, Barristers instructed as "Independent Counsel" to advices upon legal professional privilege in relation to seized material, originally issued in 2010 (last reviewed September 2023).
[130] Attorney General's Guidelines on Disclosure, updated 29 February 2024.
[131] See section 132 DPA 2018 and section 5.3 Handling confidential information below.

proceedings for that offence.[132] For these purposes, offences under the DPA 2018 are excluded.[133]

190. We can use an oral or written statement provided in response to an information notice in a prosecution for an offence under the DPA 2018 where, during any proceedings:

- in giving evidence, the person provides information inconsistent with the statement; and
- evidence relating to the statement is adduced, or a question relating to it is asked, by that person or on the person's behalf.[134]

191. Similar safeguards apply if we require a person to provide explanations or information in the exercise of our powers under warrant or if we require an individual to answer questions under an interview notice[135]

192. As an independent regulator responsible for monitoring and enforcing data protection legislation, we are not able to advise on the circumstances when the provisions about self-incrimination apply. Anyone in doubt about how the privilege against self-incrimination applies in practice should seek independent legal advice.

5.3 Handling confidential information

193. In exercising our functions, we often acquire confidential information about people and businesses.

194. There are strict rules governing the extent to which we are able to disclose this information and we must not do so without lawful authority.[136] These rules apply to the Commissioner and former Commissioners, as well as to current and former members of staff of the ICO.[137] It is a criminal offence for anyone to knowingly or recklessly disclose information in contravention of these provisions.[138]

195. Information is confidential for these purposes if:

- we have obtained it, or it has been provided to us, in the course of, or for the purpose of, discharging our functions;
- it relates to an identified or identifiable individual or business; and
- it is not available to the public from other sources at the time of the

[132] Section 143(6) DPA 2018.
[133] Section 143(7) DPA 2018. Certain other offences relating to false statements are also excluded.
[134] Section 143(8) DPA 2018. Note that these limitations do not apply to a prosecution for an offence under section 144 DPA 2018 (false statements made in response to information notices).
[135] Paragraph 16, schedule 15 DPA 2018 and section 148B DPA 2018.
[136] Section 132 DPA 2018.
[137] Section 132(1) DPA 2018.
[138] Section 132(3) DPA 2018.

disclosure and has not previously been available to the public from other sources.[139]

196. If information is confidential, we can only disclose it if:

- the individual or person carrying on the business the information relates to consents to the disclosure;
- the information was obtained for the purpose of being made available to the public;
- it is necessary in order to carry out one or more of our functions;
- it is for the purposes of criminal or civil proceedings; or
- it is necessary in the public interest, taking into account the rights, freedoms and legitimate interests of any person.[140]

197. During the course of an investigation, we may ask for representations about the confidentiality of information provided to us. We also ask for representations on confidentiality before we publish a final notice or other document, if we consider that the notice or document contains confidential information.

198. We do not accept blanket or unsubstantiated confidentiality claims and any requests for confidentiality should be accompanied by the reasons for the request. Therefore, any requests for us to keep information confidential should explain why:

- the information is considered to be confidential; and
- the proposed disclosure is not necessary for our functions or would be contrary to the rights, freedoms and legitimate interests of any person, to the extent relevant. For example, this may be because the information is commercially sensitive or contains details of a person's private affairs that, if disclosed, would be likely to significantly harm the interests of the business or person.

199. We set a reasonable deadline for representations on confidentiality before we disclose the information we have obtained. If we do not receive any representations within the time provided, we will assume the information is not considered to be confidential when deciding whether we have lawful authority to disclose it.

200. If we do not agree with a request claiming that information is confidential and decide to disclose it because we have lawful authority, we inform the person who made the request before we make the information public. It is

[139] Section 132(1) DPA 2018.
[140] Section 132(2) DPA 2018.

for us to determine what, if any, redactions it is appropriate to make prior to publication.[141]

201. For complaints, we typically share details of the complaint, including the complainant's identity, with the controller or processor for comment. If a complainant has concerns about sharing their identity with the subject of an investigation, they should raise this concern with us, ideally at the time of making the complaint. To address any concerns, we may share details about the complaint but in redacted form by removing confidential information and personal data. However, we may not be able to maintain confidentiality in all cases. For example, if the controller or processor needs this information to respond properly or make meaningful representations about any alleged infringement of data protection legislation.

5.4 Determination relating to the special purposes: journalistic, academic, artistic or literary purposes

202. We are restricted in our use of our investigatory and enforcement powers with respect to the processing of personal data for the purpose of journalism or for academic, artistic or literary purposes (referred to as the "special purposes"[142]). Therefore, if a controller or processor is processing personal data for the special purposes, we must take additional considerations into account before we can use our powers.

203. We can only give an enforcement notice or penalty notice about processing personal data for the special purposes if we first make a written determination that the personal data is not being processed:

- only for the special purposes; or
- with a view to the publication by a person of journalistic, academic, artistic or literary material that has not previously been published by the controller.[143]

204. We must give written notice of such a determination to the controller and processor (as relevant).[144] This notice must provide information about the right of appeal to the Tribunal against the determination.[145]

205. Our determination does not take effect until either:

- the period for the controller or processor to appeal against the

[141] As a public body we are subject to the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 meaning that we may have to disclose information we hold in response to an information request, subject to any relevant exemptions from disclosure. For further information, see our guidance: Freedom of information guidance and resources | ICO and Guide to the Environmental Information Regulations | ICO.
[142] The "special purposes" are defined in section 174(1) DPA 2018.
[143] Section 174(3) DPA 2018.
[144] Section 174(4) DPA 2018.
[145] Section 174(5) DPA 2018 and section 162(4) DPA 2018. On appeal, the Tribunal may cancel our determination (section 163(6) DPA 2018).

determination has ended without it bringing an appeal; or

- the controller or processor has brought an appeal against the determination and:
  - the appeal and any further appeal about the determination has been decided or has otherwise ended; and
  - the time for appealing against the result of the appeal or further appeal has ended without the controller or processor bringing another appeal.[146]

206. We can give an information notice if a determination has taken effect or if we have reasonable grounds for suspecting that such a determination could be made and we require the information for the purposes of making the determination.[147] Similarly, a judge can only give a warrant in respect of personal data processed for the special purposes if a determination with respect to the data or the processing has taken effect.[148] We cannot give an assessment notice or interview notice with respect to the processing of personal data for the special purposes.[149]

207. Once we have made a determination and it has taken effect, we can only give an enforcement notice or penalty notice for a failure by a controller or processor if a court grants leave for the notice to be given.[150] In either case, a court must not grant leave unless it is satisfied that:

- we have reason to suspect a failure by a controller or processor that is of substantial public importance; and
- the controller or processor has been given notice of the application for leave in accordance with the rules of court or the case is urgent.[151]

[146] Section 174(6) DPA 2018.
[147] Section 143(1) DPA 2018.
[148] Paragraph 3, schedule 15 DPA 2018.
[149] Section 147(5) DPA 2018 and 148B(8) DPA 2018. However, when we are conducting a review of processing of personal data for the purposes of journalism under section 178 DPA 2018, we can give an assessment notice where a determination under section 174 with respect to the data or the processing has taken effect (pursuant to paragraph 3, schedule 17 DPA 2018).
[150] Section 152(1) and section 156(1) DPA 2018. The relevant failures by a controller or processor are those described in section 149(2) DPA 2018.
[151] Section 152(2) and section 156(2) DPA 2018.

6 Deciding on the outcome of an investigation

208. We can conclude our investigations in several ways. Having assessed the evidence we have obtained during our investigation, we may decide:

- to close the investigation based on our priorities or because we have decided to resolve the issues through other means (see section 6.1 Closing investigations based on our priorities or resolving issues through other means);
- there are no grounds for action because we have not found an infringement of data protection legislation (see section 6.2 No grounds for action);
- to give a warning if we consider that a controller or processor's intended processing operations are likely to infringe data protection legislation (see section 7 Process for giving warnings)[152];
- to give a preliminary enforcement notice if our provisional view is that a controller or processor has infringed data protection legislation and we require it to remedy the infringement by taking steps, or refraining from taking steps (see section 9 Process for giving enforcement notices)[153]; or
- to give a notice of intent to impose a penalty notice or (in less serious cases) a reprimand, if our provisional view is that a controller or processor has infringed data protection legislation (see section 8 Process for giving reprimands and section 10 Process for giving penalty notices).[154]

209. The decision on the outcome of an investigation is taken by the senior leadership lead or by a separate decision maker with delegated authority under the ICO scheme of delegations, where appropriate in consultation with other senior individuals within the ICO.

210. As explained later in this guidance, if we decide to give a preliminary enforcement notice or notice of intent, we give the recipient the opportunity to make representations on our provisional findings.

211. After considering any representations, we may decide:

- to close the investigation based on our priorities or resolve the issues

[152] Article 58(2)(a) UK GDPR and paragraph 2(b), schedule 13 DPA 2018.
[153] Section 149 DPA. We can also give an enforcement notice to monitoring bodies and certification providers (see section 149(3) and (4) DPA 2018).
[154] These outcomes are not mutually exclusive and an investigation may result in a combination of a warning, preliminary enforcement notice or notice of intent to impose a penalty notice or a reprimand being given, particularly where the investigation covers multiple processing operations, or concerns both (i) previous and ongoing alleged infringements and (ii) intended processing operations likely to infringe data protection legislation.

through other means;

- there are no grounds for action if we are persuaded that our provisional view that there is, or has been, an infringement of data protection legislation is not established;
- to give an enforcement notice requiring the recipient to remedy the infringement by taking steps, or refraining from taking steps[155]; or
- to give a reprimand or (in more serious cases) a penalty notice requiring payment of a fine.

212. The decision-making process for reaching a final decision in cases where we have given a preliminary enforcement notice or notice of intent is explained in the sections below.

213. In some cases, we may accept a request by a controller or processor to settle the investigation (see section 11 Settlement procedure).

6.1 Closing investigations based on our priorities or resolving issues through other means

214. We may decide to close an investigation either before or after we have given a warning, preliminary enforcement notice or notice of intent. This may be because we decide that an investigation no longer fits our priorities or we consider it is appropriate to resolve the issues through other means.

215. As set out in section 2.4.2 Other means of resolving the issue, this may among other things include providing advice and recommendations or accepting assurances to resolve our concerns. A relevant factor we will take into account in making our assessment is whether we could allocate our resources more appropriately to other work, particularly if we would need to put in significant further effort to continue the investigation.

216. If we decide to close the investigation based on our priorities or by resolving the issues through other means, we inform the subject of the investigation about our decision in writing. We also inform any complainant that we have decided to close the investigation. In these cases, we may provide an opportunity for any complainant to comment before we finalise our decision to close the investigation.

217. If we have previously made the investigation public, we generally publish a statement on our website indicating that we have closed the investigation with a brief explanation about the basis for doing so, including if we have

[155] In some circumstances, we may require an organisation to comply with an enforcement notice urgently. See section 9 Process for giving enforcement notices.

resolved the issues through other means. The amount of detail we give varies depending on the circumstances of each case.

6.2 No grounds for action

218. If we do not find sufficient evidence of an infringement of data protection legislation, we may close a case because there are no grounds for action. We may do so either before or after we have given a preliminary enforcement notice or notice of intent.

219. In these circumstances, if we have previously made the investigation public, we generally publish a statement on our website confirming that we have closed the investigation because there are no grounds for action. We may also publish our reasons for why we have decided this.

7 Process for giving warnings

220. If we consider that a controller or processor's intended processing operations are likely to infringe data protection legislation, we may give a warning.[156]

221. A warning puts a controller or processor on notice that, if it commences its intended processing operations, we consider that it would be unlikely to comply with data protection legislation, based on the information available to us at the time of the warning. A warning does not prohibit the controller or processor from proceeding with its intended processing operations. However, the warning should encourage it to ensure its intended processing complies with data protection legislation and not to proceed until that is the case.

7.1 Giving warnings

222. In many cases, we are likely to give a warning before we open an investigation. Typically, giving a warning involves a degree of urgency. This is because it is likely to be the most appropriate intervention if we become aware of intended processing that, on the balance of probabilities, is likely to infringe data protection legislation and we need to act quickly. However, there may also be cases where we give a warning after opening an investigation. For example, if we become aware of intended processing during the course of our information gathering.

223. The decision to give a warning is taken by a decision maker with delegated authority under the ICO scheme of delegations, where appropriate in consultation with other senior individuals within the ICO.

224. A warning is preliminary by nature. It sets out our view that intended processing is likely to infringe data protection legislation and is based on the information available to us at the time. Depending on the circumstances, there may be relatively limited information available to us, especially if there is a need to act quickly. Therefore, a warning is not a formal finding that a controller or processor has infringed data protection legislation.

225. A warning sets out:

- the name, address and primary activities of the controller or processor the warning is given to;
- the relevant background to the controller or processor's decision to engage in the intended processing operations;

[156] Article 58(2)(a) UK GDPR and paragraph 2(b), schedule 13 DPA 2018.

- our understanding of the intended processing operations;
- the specific provisions of data protection legislation that we consider are likely to be infringed by the intended processing operations; and
- the reasons why we have come to this view.

226. There is no statutory requirement for us to provide a controller or processor with advance notice of our intention to give a warning or an opportunity to make representations on a proposed warning. Given the preliminary and non-binding nature of warnings, we do not generally provide notice or opportunity to make representations. However, we may do so if we consider it is appropriate in the specific circumstances of a case, including if we consider that doing so is likely to encourage the controller or processor to enter into early and meaningful engagement with us about measures to ensure its intended processing operations comply with data protection legislation.

7.3 Effect of warnings

227. A warning is not binding and does not require a controller or processor to refrain from proceeding with its intended processing operations. However, if the controller or processor still commences the relevant processing operations in a way that we consider infringes data protection legislation, we may regard its failure to take into account the warning as an aggravating factor when we are considering what, if any, steps to take.

228. This means that if a controller or processor decides to commence the intended processing operations without having appropriately addressed the concerns raised in the warning, its failure to do so could increase the likelihood of us taking enforcement action. This includes considering the controller or processor's response to the warning when deciding whether to give a notice of intent to impose a penalty notice and, if so, when deciding on the level of the proposed fine.[157]

7.4 Public announcement of warnings

229. We typically make a public announcement when we give a warning by publishing a statement on our website.

230. We may also issue a press statement or briefing to the media. We do not agree the text of our statement with the controller or processor. We provide it with the text of our statement in advance of publication and give it an opportunity to comment on any factual inaccuracies or make representations about confidentiality.

[157] Article 83(2)(i) UK GDPR and section 155(3)(k) DPA 2018. See also the Data Protection Fining Guidance, paragraphs 94 and 95.

231. At the same time as the announcement, or as soon as possible afterwards, we publish a non-confidential copy of the warning on our website. A delay in publishing the warning gives us an opportunity to seek representations from the recipient about any confidential information that may be contained in the warning (see section 5.3 Handling confidential information).

232. In some cases, we may decide not to announce publicly that we have given a warning or publish a copy of it. For example, if doing so would have a significant detrimental impact on data subjects or there are concerns about national security and defence that cannot be resolved through anonymisation or redactions.

7.5 Challenging a warning

233. A controller or processor does not have a statutory right to appeal a warning under the data protection legislation. However, a controller or processor may apply to the court for permission to challenge our decision to give a warning by judicial review.

8 Process for giving reprimands

234. Where we conclude that a controller or processor's processing operations have infringed data protection legislation, we may give it a reprimand.[158]

235. A reprimand makes a finding that the controller or processor has infringed data protection legislation, but it does not impose any legally binding obligations. Consequently, we generally give reprimands about less serious infringements of data protection legislation.[159]

236. We may give a reprimand if we consider it is an appropriate enforcement measure because it represents an effective and proportionate response to the investigation's findings. For example, this may be the case if we consider that:

- the infringement is not serious enough to require a fine, taking into account factors such as the categories of personal data affected, the number of people affected, and the level of damage suffered;
- the infringement is no longer ongoing, and we do not require the controller or processor to bring its processing operations into compliance with data protection legislation by taking any further steps, or refraining from taking steps;
- there are mitigating factors that mean it is not appropriate to impose a fine on the controller or processor;[160]
- it is in the public interest to give a reprimand, for example, to clarify important issues of data protection compliance with a view to promoting enhanced compliance practices by controllers or processors generally; or
- in accordance with our approach to public sector enforcement, a penalty notice is not appropriate in the circumstances.

8.1 Notices of intent and representations about reprimands

237. There is no statutory requirement for us to provide a controller or processor with advance notice of our intention to give a reprimand or give it the opportunity to make representations on a proposed reprimand.

238. However, because a reprimand makes a finding that a controller or processor has infringed, or is infringing, data protection law, we generally give the controller or processor with a notice of intent to give a reprimand.

[158] Article 58(2)(b) UK GDPR and paragraph 2(c), schedule 13 DPA 2018.
[159] Recital 148 to the UK GDPR states that "In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be given instead of a fine."
[160] Paragraphs 74 to 101 of the Data Protection Fining Guidance provide examples of the mitigating factors we may take into account.

This is to ensure that it knows the substance of the case against it. The notice of intent contains or refers, as necessary, to the evidence we rely on to make our provisional findings.

239. We also give the controller or processor an opportunity to make written representations on the notice of intent to give a reprimand. This ensures that the controller or processor is able to respond to and comment on the matters referred to in the notice of intent before we decide whether to give a reprimand.

240. The deadline for submitting written representations is specified in the notice of intent. We usually request a response within 21 calendar days of receipt of the notice of intent, unless the particular circumstances mean it is appropriate to give a longer period, for example in more complex cases. Where relevant, the recipient should also provide us with a non-confidential version of its representations, along with an explanation that justifies why we should treat information in its representations as confidential. The controller or processor should provide the non-confidential version within one week of the date of submitting its original response.

241. There is no obligation to submit a response to the notice of intent. If we do not receive a response before the deadline, we assume the controller or processor does not wish to make any representations and proceed to make a decision about whether it is appropriate to give a reprimand. If this is the case, we note in the decision that the controller or processor did not make representations on the notice of intent.

242. A controller or processor should make any requests for an extension to the deadline as soon as possible. The request must explain the reason why it requires an extension. In order not to delay investigations, we only give extensions to the time for submitting written representations on a notice of intent to give a reprimand if there are compelling reasons for doing so and this should not be regarded as normal practice.

243. We do not offer the controller or processor the opportunity to make oral representations in response to a notice of intent to give a reprimand. If it wishes to request this opportunity, it should explain in writing the reasons why it is needed in the circumstances of the case. This includes explaining what an oral hearing would add beyond the ability to make written representations. If we agree, we follow the process explained in section 10.3 Procedure for oral hearings.

8.2 Giving reprimands

244. The senior leadership lead takes the decision to give a reprimand, where appropriate in consultation with other senior individuals within the ICO. They consider whether there is sufficient evidence to demonstrate, on the

balance of probabilities, that a controller or processor has committed an infringement of data protection legislation and it is appropriate to give a reprimand. If we have given a notice of our intention to give a reprimand and we have received representations, the senior leadership lead carefully considers these representations before reaching their final decision.

245. If, after considering any representations and any other additional information we have obtained, the senior leadership lead decides we do not have sufficient evidence to find, on the balance of probabilities, that the controller or processor has committed an infringement of data protection legislation, we will close the case or resolve the issue through other means (see section 6 Deciding on the outcome of an investigation).

246. Alongside the reprimand, we may also provide recommendations to assist the controller or processor in ensuring that its processing does not infringe data protection legislation and to maintain compliance. These recommendations do not form part of the reprimand and are not legally binding. Therefore, any decision by the controller or processor to follow our recommendations is voluntary.

247. If a controller or processor fails to rectify the infringements set out in the reprimand, we may take that into account when deciding whether to take enforcement action about the same matter in the future. This includes when we decide whether to give a penalty notice and determine the amount of any fine that we impose.[161]

8.3 Public announcement of reprimands

248. Generally, we do not publicly announce when we send a notice of our intention to give a reprimand to a controller or processor.

249. However, we typically make a public announcement when we give a final reprimand by publishing a statement on our website. We may also issue a press statement or briefing to the media. We do not agree the text of our statement with the controller or processor. We provide it with the text of our statement in advance of publication to give it an opportunity to comment on any factual inaccuracies or make representations about confidentiality.

250. At the same time as the announcement, or as soon as possible thereafter, we publish a non-confidential copy of the reprimand on our website. A delay in publishing the reprimand provides an opportunity for us to seek representations from the recipient about any confidential information that may be contained in the reprimand (see section 5.3 Handling confidential information).

[161] Article 83(2)(i) UK GDPR and section 155(3)(e) DPA 2018. See also the Data Protection Fining Guidance.

251. In some cases, we may decide not to announce publicly that we have given a reprimand or publish a copy of it. For example, if doing so would have a significant detrimental impact on data subjects or there are concerns about national security and defence that cannot be resolved through anonymisation or redactions.

8.4 Challenging a reprimand

252. A controller or processor does not have a statutory right to appeal a reprimand under data protection legislation. However, the controller or processor may apply to the court for permission to challenge our decision to give the reprimand by judicial review.

9 Process for giving enforcement notices

253. If we decide that a controller or processor has infringed, or is continuing to infringe, data protection legislation, we may give it with an enforcement notice.[162] An enforcement notice specifies the steps we require it to take, or refrain from taking, to comply with data protection legislation.[163]

254. We can give an enforcement notice to a controller or processor if its processing operations have infringed, or are continuing to infringe, data protection legislation.[164] In summary, we can give an enforcement notice to a controller or processor about infringements that concern failing to comply with:

- the principles of processing personal data;[165]
- people's rights about the processing of their personal data;[166]
- the obligations imposed on controllers or processors, for example:
  - implementing measures to ensure the security of personal data;
  - carrying out a data protection impact assessment and consulting with us before commencing processing, where applicable; and
  - appointing a data protection officer, where applicable;[167]
- the requirement to communicate a personal data breach to us and to inform the people affected;[168]
- the principles for the transfer of personal data outside the UK;[169] and
- the requirement to pay the data protection fee.[170]

255. We can also give an enforcement notice if:

- a monitoring body charged with monitoring compliance with approved codes of conduct has failed to comply with their obligations under the UK GDPR;[171] or

[162] Section 149(1) DPA 2018. As set out in section 115 DPA 2018, various of our powers in article 58(2) UK GDPR can only be exercised by us giving an enforcement notice under section 149 DPA 2018. Article 58(2)(d) provides us with a power to order a controller or processor to bring processing operations into compliance with UK GDPR, where appropriate, in a specified manner and in a specified period.
[163] Section 149(1) DPA 2018.
[164] Note that in the case of a joint controller in respect of the processing of personal information to which part 3 or 4 DPA 2018 applies whose responsibilities for compliance with that part are determined in an arrangement under section 58 or 104, we may only give the controller an enforcement notice in reliance on section 149(2) DPA 2018 if the controller is responsible for compliance with the provision, requirement or principle in question (see section 152(4) DPA 2018).
[165] Section 149(2)(a) DPA 2018.
[166] Section 149(2)(b) DPA 2018.
[167] Section 149(2)(c) DPA 2018.
[168] Section 149(2)(d) DPA 2018.
[169] Section 149(2)(e) DPA 2018.
[170] Section 149(5) DPA 2018.
[171] Section 149(3) DPA 2018.

- a certification provider does not meet the requirements for accreditation or has failed, or is failing, to comply with obligations under the UK GDPR about the certification of organisations, or any other provision of the UK GDPR (whether in its capacity as a certification provider or otherwise).[172]

256. We can use an enforcement notice to impose any requirements that we consider appropriate to remedy the infringement of data protection legislation.[173] These requirements may include requiring a controller or processor, as appropriate, to:

- comply with a data subject's requests to exercise their rights[174];
- communicate a personal data breach to the data subject[175];
- stop processing personal data, either indefinitely or for a temporary period[176];
- rectify inaccurate personal data or erase personal data;[177] or
- suspend data flows to a recipient in a third country or to an international organisation.[178]

257. We can also use enforcement notices to withdraw a certification, or to order a certification body to withdraw or not issue a certification, if the requirements of certification are not, or are no longer, met.[179]

9.1 Factors we consider when deciding to give an enforcement notice

258. When deciding whether it is appropriate to impose requirements on a controller or processor by giving an enforcement notice, we consider the following:

- the nature of the infringement and its seriousness, including whether the infringement has caused, or is likely to cause, any person

[172] Section 149(4) DPA 2018. Where this guidance refers to a controller or processor in the context of imposing an enforcement notice that should, to the extent relevant, be taken as including a monitoring body or certification provider.
[173] Section 149(6) DPA 2018. In relation to certification providers, we can impose requirements we consider appropriate having regard to any failure (whether or not for the purpose of remedying the failure) (see section 149(7) DPA 2018). However, we cannot require a person to do something in an enforcement notice to the extent that requiring them to do it would involve an infringement of the privileges of either House of Parliament (see section 152(3) DPA 2018).
[174] Article 58(2)(c) UK GDPR.
[175] Article 58(2)(e) UK GDPR.
[176] Article 58(2)(f) UK GDPR and section 150(3) DPA 2018. The ban may relate to all processing of personal information or only to a specified description of processing of personal data. If the ban relates only to a specified description of processing, we may specify one or more of (i) a description of personal data, (ii) the purpose or manner of the processing, and (iii) the time when the processing takes place.
[177] Article 58(2)(g) UK GDPR and section 151 DPA 2018.
[178] Article 58(2)(j) UK GDPR.
[179] Article 58(2)(h) UK GDPR.

damage or distress[180];

- any aggravating or mitigating factors about the controller or processor's conduct, including whether:
  - it has taken action to remedy the infringement or mitigate any damage or distress and, if so, the effectiveness of that action;
  - we have previously raised concerns about its compliance with data protection legislation or we have previously given it a warning, reprimand, enforcement notice or penalty notice; and
  - how likely any steps required by an enforcement notice are to remedy the infringement and the extent that requiring the controller or processor to take those steps is reasonable and proportionate, taking into account the facts and circumstances of the case.

9.1.1 Considering damage or distress

259. In considering whether the infringement has caused or is likely to cause any person damage or distress, we consider the extent that it has affected people's rights and freedoms or otherwise led to them suffering, or being likely to suffer, harm. The damage or distress suffered may be physical, material or non-material.[181] It may include, but is not limited to:

- physical or bodily harm;
- psychological harm;
- economic or financial harm;
- discrimination;
- reputational harm; and
- loss of human dignity.[182]

260. In carrying out the assessment of the level of damage or distress, we take into account the fact that:

- some harms are more readily identifiable (eg financial loss or identity theft). Whereas others are less tangible and more challenging to identify or quantify (eg distress and anxiety or loss of control over personal data); and

[180] Section 150(2) DPA 2018 requires us, in deciding whether to give an enforcement notice in relation on section 149(2) DPA 2018, to consider whether the failure has caused or is likely to cause any person damage or distress.
[181] Recital 75 UK GDPR.
[182] See ICO, Overview of data protection harms and the ICO's taxonomy, April 2022. In the context of this guidance, we use the terms 'damage and distress' and 'harm' interchangeably.

- if an infringement affects a large number of people, it may result in a high degree of damage or distress in aggregate and give rise to wider harm to society, even if the impact on each person affected is more limited.

261. Our assessment of the level of damage or distress that has been caused, or is likely to be caused, is limited to what is necessary to assess its seriousness and decide whether giving an enforcement notice is appropriate. Typically, it does not involve us quantifying the damage or distress, either in aggregate or suffered by specific people. We may still give an enforcement notice when there is limited or even no evidence of actual or potential damage or distress, if we consider that it is reasonable and proportionate to do so. Our assessment of the level of damage or distress that has been caused, or is likely to be caused, does not affect any decisions a UK court may make about awarding compensation for damage suffered.[183]

9.1.2 Reasonableness and proportionality

262. In considering whether to give an enforcement notice and what requirements it is appropriate to impose, we take into account the extent that doing so is likely to be:

- effective in remedying the infringement; and
- reasonable and proportionate in the circumstances of the case.

263. This assessment of whether a requirement is appropriate depends on what options are available and the extent that each of those options is likely to be effective in remedying the infringement or mitigating the damage or distress it has caused, or is likely to cause. If we consider that a potential requirement is unlikely to be effective in remedying the infringement or mitigating the damage or distress, it is unlikely to be appropriate. We will instead impose a requirement that we consider is likely to be more effective.

264. In considering the reasonableness of giving an enforcement notice and the different requirements we may impose, we take their proportionality into account. Our assessment depends on the particular facts and circumstances of the case. It also depends on what options are available and our assessment of the effectiveness of each option.

265. In assessing whether giving an enforcement notice is reasonable and proportionate, we consider whether it, and the requirements it imposes :

[183] Article 82(1) UK GDPR and section 169 DPA 2018 provide any person who suffers material or non-material damage by reason of a contravention of the UK GDPR or the DPA 2018 respectively with the right to compensation for that damage from the controller or processor.

- are likely to be:
    - effective in achieving the aim of remedying the infringement, taking into account the purpose of the data protection legislation;
    - no more onerous than is needed to achieve that aim;
    - the least onerous effective measure, if there is a choice between more than one equally effective measure; and
- do not cause costs or other disadvantages that are disproportionate to the aim, again taking into account the purpose of the data protection legislation.

266. Our decision about whether an enforcement notice is appropriate to remedy an infringement is a matter of evaluation and judgement, involving our discretion. Our assessment involves taking into account the intrusiveness of the requirements we impose and the extent of any costs likely to be incurred by the controller or processor. For example, we may decide that it is reasonable and appropriate to require a controller or processor to take steps to comply with a person's request to exercise their rights or to comply with a specific obligation under data protection legislation. This may be the case even where there is limited, or even no, evidence of actual or potential damage or distress.[184]

267. By contrast, we acknowledge that other requirements are potentially significantly more onerous, such as imposing a ban on processing personal data or ordering the suspension of data flows. Before we require a controller or processor to take this step, we carefully weigh the likely impact on the controller or processor against the aims of the data protection legislation to ensure an appropriate level of protection for personal data. This includes taking into account any damage or distress caused, or likely to be caused, by the infringement.

9.2 Preliminary enforcement notices

268. There is no statutory requirement for us to provide the controller or processor with advance notice of our intention to give an enforcement notice or an opportunity to make representations on a proposed enforcement notice.

269. However, because an enforcement notice makes a finding that a controller or processor has infringed, or is infringing, data protection legislation, we generally give a preliminary enforcement notice. This is to ensure that the

[184] Examples of obligations on controllers and processors include, where relevant, putting in place an arrangement between joint controllers or between a controller and a processor, designating a representative in the UK, maintaining records of processing activities, implementing appropriate technical and organisational measures to ensure security of personal data, carrying out data protection impact assessments, and designating a data protection officer.

controller or processor is aware of the substance of the case against it. This includes our provisional conclusions about the alleged infringement, and the steps we propose requiring it to take to bring its processing operations into compliance with data protection legislation or remedy the alleged infringement. A preliminary enforcement notice sets out our provisional findings on the matters to be included in any enforcement notice (see section 9.4 Giving enforcement notices) and contains or refers, as necessary, to the information we rely on to make our provisional findings.

270. If we give a preliminary enforcement notice, we provide the controller or processor with an opportunity to make written representations on it. This ensures the controller or processor is able to make comments on the matters referred to in a preliminary enforcement notice before we decide whether to give a final notice and impose requirements on it.

271. We may not give a preliminary enforcement notice or offer the controller or processor the opportunity to make representations if there are exceptional circumstances that mean we need to act urgently (see section 9.3 Specifying the time for compliance and urgent enforcement notices).

272. The deadline for submitting written representations is specified in a preliminary enforcement notice. We usually request a response within 21 calendar days of receipt of a preliminary enforcement notice, unless the circumstances of the case mean that it is appropriate to give a longer period. For example, in more complex cases or where the proposed requirements in the preliminary enforcement notice are more onerous.

273. The recipient should also provide us with a non-confidential version of its representations, along with an explanation about why we should treat the information as confidential. The controller or processor should provide the non-confidential version of its representations at the same as it submits its confidential response, or as soon as possible afterwards.

274. There is no obligation for a controller or processor to submit representations in response to a preliminary enforcement notice. If we do not receive representations before the deadline, we assume that that the controller or processor does not wish to make any representations and we proceed to make a decision about whether it is appropriate to give an enforcement notice.

275. A controller or processor should make any requests to extend the deadline as soon as possible. The request must explain the reasons why it requires an extension. In order not to delay investigations, extensions to the time for submitting written representations in response to a preliminary enforcement notice are only given if there are compelling reasons for doing so, and should not be regarded as normal practice.

276. We do not typically offer the controller or processor the opportunity to make oral representations in response to a preliminary enforcement notice. If it wants this opportunity, it should explain in writing the reasons why it is needed in this case, including what an oral hearing would add beyond the ability to make written representations. We are more likely to agree in cases where the controller or processor can demonstrate that the proposed requirements are likely to have a significant impact on them. If we agree to an oral hearing, we follow the process explained in section 10.3 Procedure for oral hearings.

277. Generally, we do not publicly announce when we give a preliminary enforcement notice. However, in some cases we may decide to make a public announcement by publishing a statement on our website, if we consider it is in the public interest to do so. For example, to address public concern or speculation, or provide reassurance that we are taking appropriate action. We may also give a press statement and brief the media.

278. We do not agree the text of any statement with the controller or processor. We provide it with the text of the statement in advance of publication to give it an opportunity to comment on any factual inaccuracies or make representations about confidentiality. The statement makes clear that our findings at this stage are only provisional and are subject to representations from the controller or processor.

279. We do not publish the preliminary enforcement notice itself as it is a provisional decision, and the recipient has not had the opportunity to make representations.

9.3 Specifying the time for compliance and urgent enforcement notices

280. For each requirement in an enforcement notice, we specify the time or the period the controller or processor must comply within.[185] The proposed time or period for compliance is set out in any preliminary enforcement notice and we take into account any representations on the proposed time period before reaching a final decision.

281. We are generally required to give the recipient at least 28 calendar days to comply with any requirements in an enforcement notice.[186] However, we may give an enforcement notice with a time period of less than 28 days for compliance (an urgent enforcement notice), if we consider it is necessary for a controller or processor to comply with a requirement urgently.[187]

[185] Section 150(4) DPA 2018.
[186] Section 150(6) DPA 2018 and rule 22(1) of The Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009.
[187] Section 150(8) DPA 2018.

282. If we give an urgent enforcement notice, we are required to provide the controller or processor with a minimum of 24 hours to comply with the requirements of the notice.[188] An urgent enforcement notice contains a statement setting out our reasons why the recipient needs to comply with the requirement urgently.

283. Circumstances in which we consider it appropriate to require a controller or processor to comply with an urgent enforcement notice include where we consider that:

- on the balance of probabilities, the controller or processor has infringed, or is continuing to infringe, data protection legislation; and
- acting urgently is reasonably necessary to protect people from serious damage or distress that is either on-going or is likely to occur in the near future.[189]

284. Whether we exercise our discretion to give an urgent enforcement notice, and the time we give to comply, depends on the specific circumstances of the case. We are more likely to consider that it is appropriate to impose an urgent enforcement notice in circumstances where the requirement imposed is less onerous or is time limited. For example, communicating a personal data breach to data subjects or a temporary ban on processing to prevent data flows to a recipient in a third country. We may also give more weight to the need to act urgently if:

- there is a clear imbalance of power between the data subject and the controller; or
- the processing involves children's personal data or the personal data of other people who may be at greater risk of harm and require extra support to protect themselves.

285. Generally, we do not provide advance notice of an urgent enforcement notice. Therefore, the controller or processor does not have an opportunity to make representations before we give the urgent enforcement notice. A recipient of an urgent enforcement notice may apply to the court to disapply the urgency statement or to change the time period that it must comply with a requirement of the notice within.[190]

9.4 Giving enforcement notices

286. The senior leadership lead or a separate decision maker with delegated authority under the ICO scheme of delegations takes the decision to give an enforcement notice, where appropriate in consultation with other senior

[188] Section 150(8) DPA 2018.
[189] Section 160(6)(b) DPA 2018.
[190] Section 164 DPA 2018. See further section 12 Rights of appeal.

individuals within the ICO. They consider whether there is sufficient evidence to demonstrate, on the balance of probabilities, that a controller or processor has committed an infringement of data protection legislation and that it is appropriate to give an enforcement notice. If we have given a preliminary enforcement notice and we have received representations, the senior leadership lead or separate decision maker carefully considers these representations before reaching their final decision.

287. If, after considering any representations and any other additional information we have obtained, the senior leadership lead or separate decision maker decides we do not have sufficient evidence to find, on the balance of probabilities, that the controller or processor has committed an infringement of data protection legislation, we will close the case or resolve the issue through other means (see section 6 Deciding on the outcome of an investigation).

288. If we decide to impose an enforcement notice, it sets out:

- the relevant background facts;
- the applicable legal framework;
- the details of the infringement of data protection legislation that the enforcement notice is given about, including what the recipient of the enforcement notice has failed, or is failing, to do[191];
- confirmation of whether the controller or processor made representations in response to the preliminary enforcement notice;
- the reasons why we have decided that the controller or processor has committed an infringement[192];
- how we have considered whether the infringement has, or is likely to, cause any person damage or distress;
- the steps that we require the recipient of the notice to take or refrain from taking, or both;
- the time(s) or the period(s) that the controller or processor must comply within for each requirement imposed by the enforcement notice[193];
- information about the consequences of failing to comply with the enforcement notice,[194] which may lead to us giving a penalty notice[195]; and

[191] Section 150(1)(a) DPA 2018.
[192] Section 150(1)(b) DPA 2018.
[193] Section 150(4) DPA 2018.
[194] Section 150(5)(a) DPA 2018.
[195] Section 155(1)(b) DPA 2018.

- information about the rights of appeal.[196]

289. After we have imposed an enforcement notice, we may cancel or vary its terms by writing to the controller or processor we gave it to.[197] A controller or processor given an enforcement notice may apply to us, in writing, for the cancellation or variation of the notice.[198] However, it may only do so:

    - after the end of the period that it may appeal against the enforcement notice within; and
    - on the ground that, because of a change in circumstances, it does not need to comply with one or more of the provisions of the enforcement notice in order to remedy the infringement of data protection legislation identified in the enforcement notice.[199]

290. If the recipient wishes to apply for a cancellation or variation of an enforcement notice, it should send its written application to the senior leadership lead. The application should explain the reasons why it believes the enforcement notice should be cancelled or varied and provide evidence demonstrating the changes in circumstances.

291. We carefully consider any written requests before reaching a decision about whether to cancel or vary the enforcement notice. We consider each application on its merits. However, it is likely that we will only agree if the recipient can show that the change in circumstances is material and we are satisfied the cancellation, or variation, will not lead to damage or distress to data subjects.

292. If a recipient does not comply with a requirement in an enforcement notice, we may take enforcement action by imposing a fine (see Penalty notices). We decide how to proceed by taking into account the relevant circumstances of the failure to comply, including the reasons for, and the extent of, the non-compliance. We also consider the need to ensure an effective deterrent against recipients not complying with enforcement notices. In particular where failing to comply has:

    - led, or is likely to lead, to further damage or distress to data subjects; or
    - resulted in the recipient obtaining an advantage or benefiting from the failure.[200]

[196] Section 150(5)(b) DPA 2018.
[197] Section 153(1) DPA 2018.
[198] Section 153(2) DPA 2018.
[199] Section 153(3) DPA 2018.
[200] See also the Data Protection Fining Guidance.

293. A recipient of an enforcement notice may appeal the notice to the Tribunal. It may also appeal to the Tribunal against the refusal of an application for the cancellation or variation of an enforcement notice.[201]

9.5 Public announcement of enforcement notices

294. Typically, we publicly announce when we give an enforcement notice by publishing a statement on our website. We may also issue a press statement and brief the media. We do not agree the text of our statement with the controller or processor. We provide it with the text of our statement in advance of publication to give it an opportunity to comment on any factual inaccuracies or make representations about confidentiality.

295. At the same time as the announcement, or as soon as possible afterwards, we publish a non-confidential copy of the enforcement notice on our website. The delay in publishing the enforcement notice gives us an opportunity to seek representations from the recipient about any confidential information that may be contained in the enforcement notice (see section 5.3 Handling confidential information).

296. In some cases, we may decide not to announce publicly that we have given an enforcement notice or publish a copy of the enforcement notice. For example, if doing so would have a significant detrimental impact on data subjects or there are concerns about national security and defence that cannot be resolved through anonymisation or redactions.

[201] Section 162(1) and (2) DPA 2018. See further section 12 Rights of appeal.

10 Process for giving penalty notices

297. We can give penalty notices for:

- infringements of the UK GDPR, Part 3 DPA 2018 (Law enforcement processing) or Part 4 DPA 2018 (Intelligence services processing); and
- failing to comply with an information notice, an assessment notice or an enforcement notice given under Part 6 DPA 2018.[202]

298. We have published Data Protection Fining Guidance that sets out:

- the circumstances in which we would consider it appropriate to give a penalty notice; and
- how we determine the amount of any fine imposed.[203]

299. We can also give penalty notices for failing to comply with the requirement to pay the data protection fee.

300. This procedural guidance explains the process we follow when deciding whether to give a penalty notice.[204]

10.1 Notice of intent to give a penalty notice

301. We are required to give a written notice of intent before giving a penalty notice in order to inform the recipient that we intend to impose a fine on them.[205]

302. The notice of intent to impose a penalty notice must include:

- the name and address of the person we propose to give a penalty notice to;[206]
- the reasons why we propose to give a penalty notice,[207] including a description of the circumstances of the alleged infringement[208] and, where relevant, the nature of the personal data involved;[209] and
- an indication of the amount of the proposed fine, including any aggravating or mitigating factors that we propose to take into account.[210]

[202] Section 155(1) DPA 2018.
[203] ICO, Data Protection Fining Guidance, March 2024.
[204] It also sets out the guidance we are required to publish under section 160(7)(b) and (d) DPA 2018 about the circumstances in which we would consider it appropriate to allow a person to make oral representations and how we will determine how to proceed if a person does not comply with a penalty notice.
[205] Paragraph 2(1), schedule 16 DPA 2018.
[206] Paragraph 3(1)(a), schedule 16 DPA 2018.
[207] Paragraph 3(1)(b), schedule 16 DPA 2018.
[208] Paragraph 3(2)(a), schedule 16 DPA 2018.
[209] Paragraph 3(2)(b), schedule 16 DPA 2018.
[210] Paragraph 3(1)(c), schedule 16 DPA 2018.

303. We are likely to have obtained the information we rely on when making our decision to give a notice of intent to impose a penalty from the controller or processor. It either provided it voluntarily or we obtained it using our information gathering powers (see section 4.1 Information notices and section 4.2 Assessment notices). The notice of intent refers to the information provided by the controller or processor, where relevant.

304. In some cases, we also obtain information from third parties as part of our investigation, for example experts, complainants, data subjects, or other regulatory bodies (both within and outside of the UK). If so, we set out this information, where relevant, in the notice of intent and provide the controller or processor with access to the relevant information to the extent it is not included in the notice of intent. This material may include information that we rely on in making our provisional findings, as well as any material that, in our opinion, may undermine those findings. Subject to any confidentiality considerations, we provide copies of any relevant information from third parties not included in the notice of intent either in an annex to the notice of intent or in an accompanying document bundle. This depends on the nature and quantity of the information we are disclosing.

305. Generally, we do not publicly announce when we give a notice of intent to impose a penalty notice. However, in some cases we may decide to do so by publishing a statement on our website, if we consider it is in the public interest. For example, to address public concern or speculation, or to provide reassurance we are taking appropriate action. We may also give a press statement and brief the media.

306. We do not agree the text of any statement with the controller or processor. We provide it with the text of any statement in advance of publication to give it an opportunity to comment on any factual inaccuracies or make representations about confidentiality. The statement makes clear that our findings at this stage are only provisional and are subject to representations from the controller or processor.

307. We do not publish the notice of intent itself as it is a provisional decision, and the recipient has not had an opportunity to make representations.

10.2 Representations on a notice of intent to impose a penalty notice

308. When giving a notice of intent, we are required to inform the recipient that it may make written representations about our intention to give a penalty notice and specify the deadline to submit its representations.[211] We are

[211] Paragraph 3(3), schedule 16 DPA 2018.

required to provide the controller or processor with a minimum of 21 calendar days to make their representations.[212]

309. The deadline for submitting written representations is specified in the notice of intent. This is set on a case-by-case basis, depending on the individual circumstances, including the content of the notice of intent and the volume of information we relied on. We usually require a response within four weeks of receipt of the notice of intent. Where relevant, the recipient should also provide us with a non-confidential version of its representations, along with an explanation that justifies why we should treat the information as confidential. It should provide the non-confidential version at the same time as the confidential response, or as soon as possible afterwards.

310. The controller or processor is under no obligation to submit a response to the notice of intent. If we do not receive a response before the deadline, we assume that the recipient does not wish to make any representations and we proceed to deciding whether it is appropriate to give a penalty notice.

311. A controller or processor should make any requests for an extension to the deadline as soon as possible following receipt of the notice of intent. Its request must explain why it requires an extension. We generally only accept requests for an extension to make written representations if:

    - there are compelling reasons for providing an extension;
    - the extension will not unduly delay our investigation, particularly having regard to the requirement to give the penalty notice within six months of the notice of intent, or as soon as reasonably practicable thereafter.

312. We also consider whether it is appropriate to offer the recipient of the notice of intent the opportunity to make oral representations in response. While we exercise our discretion depending on the specific circumstances of each case, we generally offer the recipient of a notice of intent to impose a penalty notice the opportunity to make oral representations.

313. If so, the notice of intent states that the recipient may make oral representations and specifies the arrangements for making them and the time or the period that the controller or processor should make them within.[213] We arrange for oral representations to be made at a single oral hearing using the procedure set out below.

[212] Paragraph 3(4), schedule 16 DPA 2018.
[213] Paragraph 3(5), schedule 16 DPA 2018.

10.3 Procedure for oral hearings

314. While we encourage a controller or processor to take up the opportunity to attend an oral hearing, if we offer it, it is ultimately a decision for the controller or processor. The controller or processor should make clear whether they wish to do so, either before or when submitting their written representations.

315. The controller or processor may bring its legal or other advisers to the oral hearing to assist with presenting their oral representations. This is subject to any reasonable limits we may impose on the number of people attending. However, while the controller or processor may be accompanied by its legal or other advisers, we expect senior staff, directors or other decision makers within the organisation to attend and actively participate in presenting the oral representations.

316. We consider requests to hear oral hearings virtually or in a hybrid format, particularly if attendees are based outside the UK. We seek to be as flexible as we can in offering dates and times. However, we expect controllers or processors to prioritise attendance over other matters. If the lack of availability of an controller or processor's staff member or representative risks leading to a delay in our investigation, we may require it to go ahead without that person attending or we may withdraw the offer of an oral hearing.

317. The oral hearing is held after the deadline for the submission of written representations in response to the notice of intent. It is attended by the senior leadership lead, the decision maker with delegated authority under the ICO scheme of delegations, members of the case team (who may represent a range of departments within the ICO), and a representative from the ICO Legal Service. The oral hearing is chaired by the senior leadership lead or another senior ICO attendee.

318. In order to promote a focused and productive hearing, we may ask the controller or processor to provide an indication, in advance, about the matters that it proposes to focus on in its oral representations. Where possible, we agree an agenda for the oral hearing with the controller or processor in advance. The agenda generally allocates reasonable periods of time for:

    - an introduction from the chair and discussion of any preliminary matters;
    - presentation of the controller or processor's oral representations;
    - questions from us on any of the points the controller or processor raised in its written and oral representations; and
    - an indication of the next steps in the case.

319. The oral hearing provides the controller or processor with an opportunity to highlight issues of particular importance to its case that have been set out in its written representations. It may also give a useful opportunity for the controller or processor to clarify any of the details set out in its written representations, where necessary. It should limit points it raises at the oral hearing to those it has already submitted to us as part of its written representations.

320. During the oral hearing, the ICO attendees may ask questions about the controller or processor's written or oral representations. It assists us, and is likely to expedite the progress of the investigation, if the controller or processor provides full responses to any questions during the oral hearing. However, it is under no obligation to answer any questions in the oral hearing. It is also possible for the controller or processor to provide responses to the ICO's questions in writing after the oral hearing. If it indicates that it will respond to questions in writing after the oral hearing, the case team sets out those questions in writing and provides an appropriate deadline for response.

321. We take a detailed note of the oral hearing. We share this with the controller or processor afterwards. We ask it to confirm the accuracy of the note and, if necessary, identify any confidential information. If it does not agree that the note is accurate, it may provide additional submissions setting out its position and reasons for the disagreement. We consider these points, but we only make changes that are intended to correct any inaccuracies within the note.

10.4 Giving penalty notices

322. A decision maker with delegated authority under the ICO scheme of delegations (who is not the senior leadership lead) takes the decision to give a penalty notice, where appropriate in consultation with other senior individuals within the ICO. They consider whether there is sufficient evidence to demonstrate, on the balance of probabilities, that an infringement of data protection legislation has been committed and that it is appropriate to impose a fine. If so, they also decide on the amount of fine to impose.

323. Before making that decision, the decision maker carefully considers any oral or written representations made by the controller or processor in response to the notice of intent. They also take into account our Data Protection Fining Guidance. When taking the decision, they are supported by the case team and obtain legal advice from representatives of ICO Legal

Service. We do not give a penalty notice before the deadline specified in the notice of intent for the submission of oral or written representations.[214]

324. In some cases, we may gather further information after we give the notice of intent to inform our final decision. In particular, this may include requests for financial information. Given that we are required to give a final penalty notice within six months of the notice of intent or as soon as reasonably practicable thereafter, at this stage of the investigation we are more likely to use information notices and, if necessary, urgent information notices to obtain the information we need.

325. We must give the controller or processor a penalty notice, or written confirmation that we are not giving one, within six months of the notice of intent being given, or as soon as reasonably practicable thereafter[215]

326. In certain circumstances, we may require more than six months to finalise and give a penalty notice or confirm that we are not giving one. For example, this may be the case if we consider that:

- the controller or processor is responsible for delays in making its written or oral representations or in responding to our requests for information following its representations;
- the controller or processor has raised new issues or provided new information in its written or oral representations in response to the notice of intent;
- there is a material change in circumstances affecting the subject matter of the investigation or a significant external factor that impacts on the final decision; or
- reaching a final decision following the receipt of representations involves consideration of multiple or complex issues that require more time than usual for us to fully investigate and assess.

327. We will inform the controller or processor in writing as soon as possible before the expiration of the six-month period if we do require more than six months to finalise and give a penalty notice. We will also provide an indication of when we expect to take our final decision.

328. If, after considering any written and oral representations and any other additional information we have obtained, the decision maker decides we do not have sufficient evidence to find, on the balance of probabilities, that the controller or processor has committed an infringement of data protection legislation, we will close the case or resolve the issue through other means (see section 6 Deciding on the outcome of an investigation).

[214] Paragraph 4(1), schedule 16 DPA 2018.
[215] Paragraph 4 (A2), schedule 16 DPA 2018.

329. If we decide to impose a penalty notice, the final notice sets out:

- the name and address of the controller or processor it is addressed to;
- details of the notice of intent we gave to the controller or processor;
- confirmation of whether the controller or processor made oral or written representations in response to the notice of intent;
- the reasons why we are imposing the fine, including a description of the infringement and, where relevant, the nature of the personal data involved[216];
- the reasons for the amount of the fine, including details of any aggravating or mitigating factors that we have taken into account;
- details on how the controller or processor can pay the fine;
- details about the controller or processor's right to appeal against the penalty notice; and
- details about the enforcement powers we can use to force the controller or processor to pay the fine.[217]

330. The penalty notice also specifies the deadline for controller or processor to pay the fine,[218] which is not less than 28 days after the date we give the notice.[219]

331. A recipient of a penalty notice may appeal the notice to the Tribunal. They may also appeal to the Tribunal against the amount of the fine specified in the penalty notice, whether or not they also appeal against the notice.[220]

10.5 Public announcement of penalty notices

332. We publicly announce when we give a penalty notice by publishing a statement on our website. We are also likely to issue a press statement and brief the media. We do not agree the text of our statement with the controller or processor. We provide it with the text of our statement in advance of publication to give it an opportunity to comment on any factual inaccuracies or make representations about confidentiality.

333. At the same time as the announcement, or as soon as possible afterwards, we publish a non-confidential copy of the penalty notice on our website. The delay in publishing the penalty notice gives us an opportunity to seek representations from the recipient about any confidential information that

[216] Paragraph 5(2), schedule 16 DPA 2018.
[217] Paragraph 5(1), schedule 16 DPA 2018.
[218] Paragraph 6(1), schedule 16 DPA 2018.
[219] Paragraph 6(2), schedule 16 DPA 2018.
[220] Section 162(1) and (3) DPA 2018. See further section 12 Rights of Appeal.

may be contained in the penalty notice (see section 5.3 Handling confidential information).

334. In some cases, we may decide not to announce publicly that we have given a penalty notice or publish a copy of the penalty notice. For example, if doing so would have a significant detrimental impact on data subjects or there are concerns about national security and defence that cannot be resolved through anonymisation or redactions.

10.6 Variation and cancellation of penalty notices

335. After we have given a penalty notice, we may vary the amount of the fine by giving written notice to the controller or processor (a "penalty variation notice").[221]

336. A penalty variation notice specifies the penalty notice it relates to and how the relevant penalty is being varied.[222] We cannot use a penalty variation notice to reduce the period for paying the fine, increase the amount payable or vary the relevant penalty notice in a way that is detrimental to the controller or processor we gave it to.[223]

337. In the rare case that we give a penalty variation notice that reduces the level of fine below the amount that the controller or processor has already paid, we reimburse the excess amount that has been paid.[224]

338. We can also, where necessary, cancel a penalty notice by giving written notice to the controller or processor we gave it to.[225] If we cancel a penalty notice, we cannot give another penalty notice about the same infringement and we will repay any amount that had previously been paid due to the cancelled penalty notice.[226]

339. A controller or processor we give a penalty variation notice to may appeal to the Tribunal against the amount of the penalty specified, whether or not it has appealed against the penalty notice.[227]

10.7 Recovery of the fine

340. If the controller or processor fails to pay a fine after we give a penalty notice, we take action to recover the fine. For example, we apply to the court for an order that enforces the obligation to pay the fine.[228] We may also petition for the winding up of a company, or a person's bankruptcy; participate in insolvency proceedings as an active creditor; and share

[221] Paragraph 7(1), schedule 16 DPA 2018.
[222] Paragraph 7(2), schedule 16 DPA 2018.
[223] Paragraph 7(3), schedule 16 DPA 2018.
[224] Paragraph 7(4), schedule 16 DPA 2018.
[225] Paragraph 8(1), schedule 16 DPA 2018.
[226] Paragraph 8(2), schedule 16 DPA 2018.
[227] Section 162(1) and (3) DPA 2018. See further section 12 Rights of appeal.
[228] Paragraph 9(2) to (4), schedule 16 DPA 2018.

information and collaborate, where relevant, with external bodies, such as the Insolvency Service.

341. We cannot apply for such an order until:

- the period for payment specified in the penalty notice has ended;[229] or
- the appeal process has been decided or otherwise ended, if the controller or processor has appealed against the penalty notice, the amount of the fine, or any relevant penalty variation notice.[230]

342. Where appropriate, we may agree to provide additional time for the controller or processor to pay the fine or to allow it to pay in instalments.[231]

[229] Paragraph 9(1)(a), schedule 16 DPA 2018.
[230] Paragraph 9(1)(b)-(d), schedule 16 DPA 2018.
[231] See further: The ICO's work to recover fines.

11 Settlement procedure

343. In some cases, we may consider it is appropriate to settle an investigation. Settlement is a voluntary process where a controller or processor under investigation admits that it has infringed the data protection legislation and confirms that it accepts that a streamlined administrative procedure will govern the remainder of our investigation. If so, we impose a reduced fine on the controller or processor to reflect the early resolution of the case and resource savings involved, including those resulting from the controller or processor accepting that it will not appeal the penalty notice to the Tribunal.

344. Controllers or processors we are investigating are not under any obligation to enter into the settlement process or, if they do begin discussions, to then agree to settle. In particular, we do not regard any decision by a controller or processor not to enter into settlement discussions or to withdraw from the settlement process as an infringement of its obligation to cooperate with us.[232] We decide to settle cases at our discretion and the settlement process set out in this guidance does not preclude us from resolving investigations by other means if we consider it is appropriate to do so (see section 6.1 Closing investigations based on our priorities or resolving issues through other means).

11.1 When settlement may be appropriate

345. We may consider settlement is appropriate in any investigation into a suspected infringement where we consider we have a sufficient basis to give a notice of intent to impose a penalty notice. This follows the process set out in this guidance and takes into account our Data Protection Fining Guidance. We may consider settlement is appropriate either before or after giving a notice of intent.

346. Any decision by us to enter into settlement discussions or settle a case is entirely at our discretion. There is no right for any controller or processor to require us to enter settlement discussions or to settle a case, or any corresponding obligation on us to do so.

347. We consider whether to enter settlement discussions on a case-by-case basis, taking into account:

- whether we have sufficient evidence to impose a penalty notice;
- the procedural efficiencies and resource savings that we consider we are likely to achieve;
- how likely it is that the case will be settled in a reasonable timeframe; and

[232] See article 31 UK GDPR and section 63 DPA 2018.

- any impact on related matters.

348. When considering whether the case will be settled in a reasonable timeframe, we take into account the six month period are required to give a penalty notice within. We are unlikely to agree to settlement after giving a notice of intent if we consider it is likely to delay the outcome of the case.

349. We may decide that a case is not suitable for settlement for a range of reasons, including:

- for public policy reasons (eg if there is a high degree of harm to people caused by the infringement or there is evidence the infringement was committed intentionally);
- as a result of the attitude and conduct of the controller or processor during the investigation (eg if it has been obstructive or failed to co-operate with us); or
- the indication from the controller or processor that it is willing to settle comes at a late stage in the investigation or we consider that the resource savings from settlement are likely to be limited.

11.2 The requirements for settlement of a case

350. Before we agree to any settlement, we require at a minimum the controller or processor to:

- make an admission about the nature, scope and duration of the infringement. The scope of the infringement includes, as a minimum, the material facts of the infringement, as well as its legal characterisation. As part of the settlement, the controller or processor must agree to make no further representations on these issues;
- cease the infringing conduct immediately from the date that it enters into settlement discussions, if it has not already done so;
- accept that there will be a formal and published decision against it setting out our finding of infringement. In settlement cases we typically give shorter decisions than cases where our findings are contested (see section 11.4.4 Conclusion of the settlement process); and
- confirm it will:
    - pay a fine amount to be determined as part of the settlement process (see section 11.3 The discounts available for settling a case), the level of the reduction we give will reflect whether the settlement is being entered into before or after we have given a notice of intent;

- not subsequently seek to challenge or appeal against the findings of infringement or amount of fine in any final penalty notice we impose; and
- take any steps needed to comply with relevant provisions in the data protection legislation or remedy the consequences of the infringement.

351. We also require the controller or processor to accept a streamlined decision-making process in order to achieve our objective to resolve the case efficiently. We decide this on a case-by-case basis, taking into account this guidance, depending on the stage the settlement process is commenced at. Depending on the circumstances, it may mean the controller or processor is required to agree that it:

- does not receive a notice of intent;
- does not make written representations (except about clear and obvious factual inaccuracies); and
- has no opportunity to make representations at an oral hearing.

352. In some circumstances we may identify additional pre-requisites to settlement, such as requiring a controller or processor to assist us in any investigation into related issues or to agree to implement measures to improve compliance or provide redress for any damage or distress people may have suffered.

353. The controller or processor's decision to settle is voluntary and should be based on a full understanding of the requirements and consequences of settlement. A controller or processor may withdraw from settlement discussions at any time before confirming in writing its acceptance of the requirements for settlement.

11.3 The discounts available for settling a case

354. If the settlement process is concluded successfully, the penalty notice contains a fine amount that includes a discount for settlement. The settlement discount is applied after we have calculated the fine amount, taking into account our Data Protection Fining Guidance.

355. The level of the discount available depends on what stage of the investigation the controller or processor enters into settlement discussions. The earlier the settlement process is started, the greater the level of settlement discount available to reflect the increased resource savings.

356. We consider the settlement discount on a case-by-case basis, up to the following maximum amounts:

- 40% if a case is settled before we give a notice of intent;
- 30% if a case is settled after we give a notice of intent but before we receive written representations; and
- 20% if a case is settled after we give a notice of intent and after we receive written representations.

357. If we are concerned that the settlement process is not progressing as quickly as possible because of delays caused by the controller or processor or we consider it is not co-operating fully with the process, we may decide to bring the process to an end or reduce the available discount (based on the time taken and the use of our resources). If so, we give the controller or processor notice that we are minded to do this before taking that decision.

358. The discounts available for settlement are separate from our consideration of mitigating and aggravating factors under our Data Protection Fining Guidance. We apply any settlement discount at the conclusion of the penalty setting process, once we've considered all other factors. We do not regard engaging in settlement discussions (or choosing not to engage in settlement discussions) as either an aggravating or a mitigating factor when we decide whether to impose a penalty or the amount of any fine.

11.4 The process for settlement discussions and concluding the case

359. If the subject of an investigation wishes to discuss settlement, it should approach us by contacting the case lead or senior leadership lead. It can initiate settlement discussions either before or after we give a notice of intent. The stage of the investigation that it initiates settlement discussions affects the amount of settlement discount that is available (see section 11.3 The discounts available for settling a case).

360. If, having been approached in this way, we decide that the case is appropriate for settlement, we confirm this with the subject of the investigation and commence settlement discussions. If settlement discussions have begun before we give a notice of intent, a decision maker with delegated authority under the ICO scheme of delegations (who is not the senior leadership lead) will decide on whether to proceed with settlement, where appropriate in consultation with other senior staff of the ICO. If settlement discussions begin after we have given a notice of intent to impose a penalty notice, the decision maker who decided to give the notice of intent will decide whether to proceed with settlement.

361. We set a timetable for settlement discussions. This is important in ensuring we can achieve our goals of procedural and resource efficiencies that come

from following a streamlined process. The timetable is not a fixed duration and depends on the facts of each case (such as how early the settlement discussions began and the stage of the investigation).

11.4.1 Settlement before a notice of intent

362. If we start settlement discussions before we give a notice of intent, we provide the subject of the investigation with a statement of facts setting out the basis we are proceeding on. We also provide an indication of:

- the level of fine that we are minded to impose;
- how we would calculate the fine amount following the Data Protection Fining Guidance; and
- the level of settlement discount we would be likely to award.

363. If the controller or processor wishes to pursue settlement on the basis of the statement of facts, we give it the opportunity to provide comments on them. These are limited to identifying clear and obvious factual inaccuracies. If the comments go beyond factual corrections, we may reassess whether the case remains suitable for settlement. We also allow comments on the proposed fine amount and settlement discount, which we take into account in reaching our decision.[233]

364. If the subject of the investigation is not prepared to agree settlement on the basis of the statement of facts and proposed fine amount, we withdraw from the settlement process and proceed with the investigation. This may include preparing to give a notice of intent. Although this does not preclude the controller or processor from settling at a later stage in the process, the discount for settlement is then lower.

11.4.2 Settlement after a notice of intent and before written representations

365. If settlement discussions commence after we have given a notice of intent, but before we have received written representations, we provide an indication of the settlement discount that we would be minded to apply if the case is settled. We then set a short deadline for the controller or processor to indicate its willingness to settle and give it the opportunity to indicate any clear and obvious factual inaccuracies in the notice of intent. Again, if these comments go beyond factual corrections, we may reassess whether the case remains suitable for settlement. We also take into account any comments made on the proposed fine amount and settlement discount in reaching our decision.

[233] Where a case is settled before a notice of intent is given, the statement of facts is deemed to be the notice of intent for the purpose of schedule 16, paragraph 2(1) DPA 2018.

11.4.3 Settlement after a notice of intent and after written representations

366. A controller or processor may still indicate that it wishes to enter a settlement process after making written representations on the notice of intent. If so, in line with our usual process, we consider any written representations, including about the amount of the fine. We take the representations into account before deciding to engage in settlement discussions.

367. If we consider that it is appropriate to engage in settlement discussions despite the late stage of the investigation, we provide an indication of our thinking about the infringement, the level of fine and the settlement discount.

368. We then set a short deadline for the controller or processor to indicate its willingness to settle.

11.4.4 Conclusion of the settlement process

369. If the settlement discussions are successful and the controller or processor is prepared to accept the requirements for settlement, it must provide written confirmation of its acceptance. This must include an admission about the nature, scope and duration of the infringement. A senior member of the controller or processor who is authorised to bind it should provide the written acceptance.

370. If settlement discussions are successful, the decision to give a settlement penalty notice is taken by the decision maker with delegated authority under the ICO scheme of delegations, where appropriate in consultation with other senior individuals within the ICO. The process we follow is the same as for giving penalty notices (see section 10.4 Giving penalty notices).

371. Penalty notices we give following a successful settlement process are generally shorter than in cases where our findings are contested. The earlier in the investigation that settlement is agreed, the shorter the penalty notice is likely to be. However, in settlement cases, the penalty notice still sets out the details described in section 10.4. This includes a description of the infringement and the reasons for the amount of the fine. The penalty notice also refers to the fact that the case has been settled and sets out details of the settlement discount.

11.5 Withdrawal from the settlement process

372. A controller or processor may withdraw from settlement discussions at any time. We may also choose to end settlement discussions at any time at our discretion. We give the controller or processor prior notice of our intention

to end discussions and allow it the opportunity to comment before we take our decision to withdraw from the settlement process.

373. If settlement discussions are not successful, we continue the investigation following our usual procedure, but with a different decision maker with delegated authority under the ICO scheme of delegations appointed to take the final decision about whether to give a penalty notice. We do not consider the fact that the controller or processor has entered settlement discussions and failed to agree a settlement as either a mitigating or aggravating factor in assessing what enforcement action we may take. The content of the settlement discussions will not be revealed to the new decision maker appointed after those discussions have ended. However, the new decision maker may be aware of the fact that the possibility of settlement has been discussed.

374. Settlement discussions are conducted on an open (not "without prejudice") basis. Therefore, we may use any documents or information a controller or processor provides to us during the settlement discussions in any existing or new regulatory action, even if the settlement process is unsuccessful.

11.6 Public announcements during or after settlement

375. We do not comment publicly on the fact that settlement discussions are taking place, or that settlement discussions have been unsuccessful. Similarly, a controller or processor must not disclose the content of settlement discussions, or the fact that those discussions have taken place, to any third parties without our prior written approval.

376. If the settlement discussions are successful and we give a penalty notice, we publicly announce the circumstances as described in section 10.5 Public announcement of penalty notices and follow the same process.

12 Rights of appeal

377. A controller or processor that is given an information notice, an assessment notice, an enforcement notice, a penalty notice or a penalty variation notice, has the right of appeal to the Tribunal.[234]

378. The practice and procedure for an appeal is set out in the First-tier Tribunal rules.[235] A recipient must start an appeal within 28 days of the date the notice was sent to it.[236] The burden of proof in an appeal lies on the appellant.[237]

379. In determining the appeal, the Tribunal may review any determination of fact that the notice or decision was based on.[238]

380. The Tribunal must allow the appeal or substitute another notice or decision that the Commissioner could have given or made, if it considers:

- the notice or decision that the appeal is brought against is not in accordance with the law; or
- the Commissioner ought to have exercised their discretion differently, to the extent that the notice or decision involved an exercise of discretion by the Commissioner. [239]

381. Otherwise, the Tribunal must dismiss the appeal.[240]

382. If an information notice, an assessment notice or an enforcement notice contains an "urgency statement",[241] the recipient may apply to the court[242] for either, or both, of the following:

- the disapplication of the urgency statement about some or all of the requirements of the notice; and
- a change to the time or the period that it is required to comply with the notice within.[243]

383. The decision of the court on such an application is final.[244]

---

[234] Section 162(1) DPA 2018.
[235] Rule 22 of The Tribunal (First Tier Tribunal) (General Regulatory Chamber) Rules 2009
[236] Rule 22(1)(b) of The Tribunal (First Tier Tribunal) (General Regulatory Chamber) Rules 2009
[237] See Doorstep Dispensaree Limited v The Information Commissioner [2024] EWCA Civ 1515, paragraphs 39 to 41.
[238] Section 163(2) DPA 2018.
[239] Section 163(3) DPA 2018.
[240] Section 163(4) DPA 2018.
[241] In relation to an information notice, a statement under section 142(7)(a) DPA 2018; in relation to an assessment notice, a statement under section 146(8)(a) or (9)(d)DPA 2018; and in relation to an enforcement notice, a statement under section 150(8)(a) DPA 2018.
[242] The jurisdiction conferred on a court by section 164 DPA 2018 (applications in respect of urgent notices) is exercisable only by the High Court or, in Scotland, the Court of Session (section 180(5) DPA 2018).
[243] Section 164(2) DPA 2018.
[244] Section 164(4) DPA 2018.

384. Controllers, processors and others (provided they have sufficient interest in the matter) may challenge by judicial review other decisions we take (eg giving warnings or reprimands).