Information Commissioner's Office

Draft

Statutory guidance on our regulatory action

Pursuant to our obligations under s160 DPA 2018

ico.
Information Commissioner's Office

Contents

Foreword

We will insert a foreword here in the final version of the statutory guidance.

About this guidance

What is the purpose of this guidance?

The mission of the Information Commissioner's Office (ICO) is to uphold information rights for the UK public in the digital age. This statutory guidance sits alongside our regulatory action policy (RAP) which together set out how the ICO carries out this mission.

The RAP sets out our general approach when using our regulatory powers under the range of legislation we monitor and enforce (specifically, for the regimes that do not carry a legal obligation for formal guidance). It is split into two parts; Part A and Part B. Part A focuses on our role and explains how we:

- promote best practice and ensure compliance;
- approach our regulatory responsibilities;
- assess the outcomes of our regulatory action; and
- work with other regulators.

Part B focuses on the individual pieces of legislation we are responsible for and our specific enforcement powers for each piece of legislation.

We are issuing this statutory guidance to comply with our obligations under sections 160, 158 and 133 of the Data Protection Act 2018 (DPA 2018). It focuses on our data protection responsibilities and provides guidance on how we exercise our regulatory powers when issuing information notices, assessment notices, enforcement notices and penalty notices (s160), including fixed penalties (s158). It also details our approach to accessing privileged information (s133).

In line with our statutory obligations, this document's purpose is to provide clarity to those we regulate and the public about our approach to exercising our regulatory powers. This also helps us to achieve the goals we set out in our strategic plan.

We can take a range of regulatory actions for failures in respect of the following legislation:

- Data Protection Act 2018 (DPA 2018); and
- UK General Data Protection Regulation (UK GDPR).

We refer to these as 'data protection legislation' in this document. The relevant regulatory actions include the issuing of information notices, assessment notices, enforcement notices and penalty notices.

What does the guidance cover?

This document sets out our risk-based approach to taking regulatory action against organisations and members of the public who breach the provisions of data protection legislation. Our focus is on the areas which pose the highest risk and could cause the most harm. We set out below the principles we apply in exercising our powers.

Our approach aims to help create an environment that protects the public, while ensuring that organisations are able to operate and innovate efficiently in the digital age. We are as robust as we need to be in upholding the law, whilst ensuring that commercial businesses, charities and public services are not worried that we may use our sanctions disproportionately. We work with others, for example other regulators, where it makes sense to do so, including where it is necessary to achieve better outcomes or protections for the public.

Alongside the RAP, and to maintain an effective and proportionate regulatory response, this guidance seeks to:

- set out the nature and scope of our various statutory powers and to be clear and consistent about when and how we use them;
- ensure that we take fair, proportionate and timely regulatory action to guarantee that we properly protect the public's information rights; and
- assist in the delivery of the goals set out in our strategic plan and uphold information rights effectively for the public in the digital age.

Who is this guidance for?

This guidance is to inform both people and organisations who collect, use, store and share information about how we use our statutory powers to investigate and enforce UK data protection legislation.

Which statutory obligations does the publication of this guidance fulfil?

By issuing this document, we are fulfilling our statutory obligations to:

- provide guidance as to how we propose to exercise our powers in connection with information notices, assessment notices, enforcement notices and penalty notices (section 160(1) DPA 2018);
- provide guidance as to how we propose to ensure that we only use or disclose privileged communications (which we obtain or have access to in the course of carrying out our responsibilities) when it is necessary for carrying out our responsibilities (section 133(1)(a) DPA 2018);
- provide guidance on how we propose to comply with restrictions and prohibitions on obtaining or having access to privileged communications which an enactment imposes (section 133(1)(b) DPA 2018); and

- produce and publish a document specifying the penalty amount for a failure to pay the data protection fees, which section 137 of the DPA 2018 requires (see section 158 DPA 2018).

What is the status of this guidance?

We must produce guidance on how we use our statutory powers. Following our obligations set out in sections 158(5) and 160(9), in producing this document we consulted with ICO colleagues and ran a formal public consultation. We carefully considered the outcome of this consultation and made appropriate amendments to this policy before sharing the policy with Parliament for approval. We will keep this guidance under review to ensure it remains relevant and accurate.

What regulatory activity does this guidance cover?

Our regulatory activity includes:

- seeking information about compliance with data protection legislation by:
    - issuing information notices under section 142(1) of the DPA 2018;
    - issuing information notices with an urgency statement under section 142(7) of the DPA 2018, requiring a person or organisation to provide information on not less than 24 hours' notice;
    - applying for a court order requiring compliance with the information notice we issue under section 145 of the DPA 2018, if the recipient does not provide a full and timely response;
- conducting assessments of compliance with data protection legislation by:
    - issuing assessment notices under section 146(1) of the DPA 2018;
    - issuing assessment notices with an urgency statement under section 146(8) of the DPA 2018, requiring organisations to allow us to undertake an assessment of whether they comply with data protection legislation, on not less than seven days' notice;
    - issuing assessment notices with an urgency statement giving less than seven days to comply under section 146(9) of the DPA 2018, where we have reasonable grounds to suspect that the organisation or person:
        - failed or is failing to comply with certain provisions of the data protection legislation (set out in section 149(2) DPA 2018); or
        - committed or is committing an offence under the DPA 2018, allowing us to undertake an assessment on less than seven days' notice;
- enforcing data protection legislation by:
    - issuing enforcement notices under section 149(1) DPA 2018 requiring specific actions by a person or organisation to resolve

breaches of applicable information rights obligations;

- issuing an enforcement notice with an urgency statement under section 150(8) the DPA 2018, which we may use to require action to resolve breaches or potential breaches of data protection legislation, on not less than 24 hours' notice;
- administering fines by penalty notices in the circumstances that section 155 of the DPA 2018 sets out;
- administering fixed penalties for failing to meet specific obligations (eg paying the relevant service fee to us); and
- prosecuting criminal offences before the courts.

We provide guidance to organisations and the public about how to comply with the law. We also provide guidance in the form of:

- letters of advice;
- compliance meetings;
- presentations;
- conferences;
- advice sessions;
- our helpline;
- live chat; and
- our website.

We set out the full range of our enforcement powers, together with the regulatory actions associated with these powers and the legislation we monitor and enforce, on our website.

Further reading

Guide to Data Protection | ICO

Guide to the UK General Data Protection Regulation (UK GDPR) | ICO

Strategic plan [this document will be updated in due course]

ICO prosecution policy statement about the prosecution of offences primarily under the Data Protection Act 1998, Data Protection Act 2018, and Freedom of Information Act 2000. Last published in May 2018.

Regulatory action policy (RAP)

The ICO provides a range of guidance about data protection and the UK GDPR on our website. Visit ico.org.uk for full details.

Information notices

What is an information notice?

An information notice is a written request from the Commissioner to an organisation, requiring them to provide the Commissioner with specific information we need to carry out any of our statutory functions. We can also serve an information notice on any person or organisation, requiring them to provide information to assist with the Commissioner's investigations. Information notices may require the information to be provided within a specified time frame.

When would we issue an information notice?

When exercising our discretion whether to serve an information notice, we consider what action is appropriate and proportionate, including:

- a person or organisation's history of compliance (or non-compliance) with requests for information made in correspondence prior to serving an information notice;
- the potential risk of harm to the public or level of intrusion into their privacy that the events or data processing under investigation poses, for example where:
    - our attempts to obtain information through other alternative means fail, including by correspondence and co-operation;
    - the processing appears to be high risk or involve high risk categories of personal data; or
    - the Commissioner has reasonable doubts about the degree of co-operation they can expect from the person or organisation;
- the necessity of requiring a formal response within a defined time period;
- whether a formal response is necessary because the person or organisation has a history of non-compliance with our informal requests for information; and
- the public interest in the response.

How long do we normally give recipients to respond?

We normally give recipients of information notices at least 30 days to provide the information we require. In some circumstances we may give recipients longer to respond. When deciding the period for compliance with information notices, we consider the following:

- how urgent the requirement for the information is;
- the volume and complexity of the information we require;
- how easy it is for the person or organisation to collate the information we

require; and

- the resources available to the person or organisation responding to the information notice.

When would we issue an urgent information notice?

We may also issue an information notice on an urgent basis. The shortest period for compliance is 24 hours. When considering whether to issue an information notice with an urgency statement, and what time period we give for compliance, we consider what action is appropriate and proportionate, including:

- the extent to which urgent investigation may prevent or limit the risk of serious harm to the public or serious intrusion into their privacy;
- the extent to which urgent investigation may prevent the sanitisation, alteration, destruction, concealment, blocking, falsifying or removal of relevant evidence related to the data processing;
- the scope of the questions or requests in the information notice;
- the additional burden on the recipient in having to urgently comply with a notice and the reasonableness of that burden, taking into account all of the relevant circumstances;
- the impact on the recipient's rights should we urgently gain access to their premises and data processing activities, without or on short notice, and without the opportunity to either appeal, for the Information Tribunal to hear an appeal, or both;
- the length of time of the investigation. For example, it may not be appropriate and proportionate to issue an urgent information notice during a long running investigation; and
- the comparative effectiveness of us exercising this power instead of our other investigatory powers.

What action can we take if a person or organisation does not respond to an information notice on time?

If a recipient of an information notice does not fully respond to the notice or respond at all within the applicable timeframe, we may promptly apply to the court for an information order requiring a response. We may do so even in non-urgent cases, if it is necessary in order to progress an investigation. In deciding whether such action is necessary, we consider all the relevant circumstances. These include:

- whether the recipient partially complied with the information notice and the importance and relevance of any outstanding information to our consideration of their processing;
- any reasons they give for non-compliance with the information notice;
- any commitments they give to responding to the information notice within

a revised timeframe;

- whether the person or organisation obtained or was likely to have obtained the information from another source;
- the comparative effectiveness of our other investigatory and enforcement powers. For example, we may decide we have sufficient evidence to move to an enforcement action in any event; and
- the public interest.

We can also consider whether to issue an assessment notice or a penalty notice (see below).

In response to an information notice (under section 144 of the DPA 2018) it is an offence to:

- make a statement which the person knows to be false in a material respect; or
- recklessly make a statement which is false in a material respect.

Right of appeal

Under section 162 of the DPA 2018, recipients of information notices may appeal to the Tribunal. For the appeals procedure, please refer to The Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules.

Under section 164 of the DPA 2018, recipients of urgent information notices may apply to the court to disapply the statement of urgency or to change the time period for compliance.

Section 142(8) of the DPA 2018 allows us to cancel an information notice at any point. If we decide to cancel an information notice, we would provide written confirmation of this decision.

Further reading

Information Notices DPA 2018 (Sections 142 - 145)

Destroying or falsifying information and documents (Section 148 DPA 2018)

General Regulatory Chamber tribunal procedure rules - GOV.UK (www.gov.uk)

Assessment notices

What is an assessment notice?

An assessment notice is a written notice we may issue to a person or organisation requiring them to allow us to assess whether they complied or are complying with data protection legislation. The notice may, for example, require the person or organisation to give us access to their premises and specified documentation and equipment. In some circumstances, it may be a criminal offence to provide a false response to an assessment notice.

When would we issue an assessment notice?

We exercise our discretion to issue an assessment notice in a way which is appropriate and proportionate. In deciding whether to exercise our power, we would take into account all relevant circumstances, including whether:

- we have evidence that indicates that the person or organisation did not comply or is not complying with data protection legislation when processing personal data. We may obtain that evidence through our supervisory and regulatory activity, including the receipt of any complaints from the public. We may also obtain it from news reports, statutory reporting or publications about the organisation or person;
- there is evidence from, for example the sources listed above, that any potential non-compliance gives rise to a likelihood of damage or distress to the public;
- it is necessary to verify compliance with an enforcement notice; and
- the person or organisation failed to engage with us or respond to an information notice within an appropriate time, or the information provided to the Commissioner in response to an information notice suggests that they are not complying with data protection legislation.

When would we issue an assessment notice with an urgency statement?

In certain circumstances an assessment notice can include an urgency statement requiring a person or organisation to do something before the end of the appeal period.

Normally an urgency statement does not require compliance in less than seven days. However, we can require a person or organisation to comply with a requirement in less than seven days where we reasonably expect that they failed or are failing as described in section 149(2) DPA 2018, or that they committed or are committing an offence under the DPA 2018, and the requirement does not relate to domestic premises.

When deciding whether we need an urgency statement, we decide what action is appropriate and proportionate. We base this upon, but not limited to, the following considerations:

- the extent to which urgent investigation may prevent or limit the risk of serious harm to the public or serious intrusion into their privacy;
- the extent to which urgent investigation may prevent the sanitisation, alteration, destruction, concealment, blocking, falsifying or removal of relevant evidence of data processing;
- the scope of our requests in the assessment notice;
- the additional burden on the recipient in having to urgently comply with a notice;
- the impact on the recipient's rights should we urgently gain access to their premises and data processing activities, and without the opportunity to either appeal or for the Information Tribunal to hear an appeal or both; and
- the comparative effectiveness of our other investigatory powers.

Where we include an urgency statement, the assessment notice sets out our reasons for including the statement and, where appropriate, the nature of any suspected failures or offences.

What action can we take if an organisation or person fails to respond to an assessment notice?

We would decide whether to ask the court to issue an order requiring the person or organisation to supply the information requested. We may also apply for a warrant to gain access to their premises to obtain the information we require.

If a person or organisation fails to comply with an assessment notice, we would then consider whether to issue a penalty notice (see below).

What can we obtain or view as part of our assessment?

The assessment notice may specify documents, information or classes of documents or information which relate to how a person or organisation sought to meet their obligations under data protection legislation. It may also specify what governance controls they have in place to monitor and measure compliance. We may require access to and an opportunity to inspect, examine or copy the specified documents.

Although not an exhaustive list, the specified documents could include:

- strategies;
- policies;
- procedures;

- guidance;
- codes of practice;
- training material;
- protocols;
- frameworks;
- memoranda of understanding;
- contracts;
- privacy statements;
- privacy impact assessments;
- data protection impact assessments;
- control data;
- breach logs; or
- job descriptions.

It is a criminal offence under section 148(2) of the DPA 2018 for a person in receipt of an assessment notice to destroy, dispose of, conceal, block or falsify information, documents, equipment or material with the aim of preventing the Commissioner's access.

Access to personal or sensitive documents and information as part of an assessment

The documents we specify in the assessment notice may include information which may be regarded as sensitive. For example, personal data, commercially sensitive information or information that may engage national security concerns.

We may need to view documents and information concerning a person's physical or mental health and documents which concern the provision of a person's social care. This may include documents and information in health and social care records.

In all cases, we would access the minimum amount of information we need to assess whether the organisation or person is handling personal data appropriately.

In certain specific cases, in view of the particular sensitivity of the material, we can implement the following additional measures:

- In respect of information concerning a person's physical or mental health and documents which concern the provision of a person's social care; we would not take the content of these documents off-site, nor would we copy or transcribe them into working notes, unless:
    - we require them for evidential purposes;
    - we are considering further regulatory action; or

    - we are alerting the organisation to a potential issue that requires rectification.

  We would not include any personal data of this type in any reporting of the assessment.
- We recognise that there might also be legitimate concerns about other information which relates to issues of national security, international relations or sensitive activities. If appropriate, we may assess compliance without looking at this type of information. Where it is necessary and appropriate, we ensure that only appropriately vetted staff inspect such sensitive information. We have memoranda of understanding with relevant agencies to provide access to and explanations of this type of material.

What happens if the recipient wishes to raise questions or concerns about the access to the information we request?

A person or organisation can contact us if they wish to bring to our attention, or ask questions about, any particular aspects of personal or other sensitive information which we specify in an assessment notice. As stated above, we would only access the minimum amount of information we need to assess whether the person or organisation is handling personal data appropriately. A person or organisation may request particular access conditions. We try to accommodate such requests if we are satisfied that doing so would not compromise the effectiveness of our assessment. A person or organisation must make these requests as soon as possible.

What about inspection and examinations during assessments?

Inspections and examinations of processing on a person or organisation's premises may be key elements of an assessment. They allow us to witness and assess in practice whether a person or organisation is complying with the data protection legislation, as well as their own data policies and procedures.

We use such inspections and examinations to evaluate how a person or organisation:

- obtains, stores, organises, adapts and alters information or personal data;
- ensures the confidentiality, integrity and availability of the data or service they provide;
- retrieves, consults or uses the information or personal data;
- discloses or shares personal data by transmitting, disseminating or otherwise making the data available; and
- applies retention periods to, and disposes of, personal data.

In our review of the processing of personal data, and any associated audit trails which are available, we may consider:

- both manually and electronically stored data, including data the organisation or person stores centrally, locally, on mobile devices and media;
- management or control information, to monitor and record how an organisation or person is processing personal data and meeting their wider obligations under the legislation; and
- physical and IT-related security measures, including how an organisation or person stores and disposes of personal data.

Our review and evaluation process may take place on site as part of a discussion with staff to demonstrate 'practice', or independently by way of sampling. If the organisation or person holds information electronically, we may require them to provide manual copies or facilitate direct access. Any direct access would be:

- limited to the identified records;
- only done locally; and
- for a limited and agreed time.

If we review data as part of the evaluation process that we did not specifically identify in the assessment notice, we would only take it off the person or organisation's site with their permission.

What about interviews that we carry out during assessments?

Interviews consist of discussions with:

- senior staff and any board members;
- staff and contractors;
- any relevant person or organisation's staff; and
- staff of relevant service providers as the assessment notice specifies.

We conduct interviews to develop our understanding of working practices in connection with data processing and the levels of awareness amongst relevant personnel of organisation's regulatory obligations. We may interview, for example, departmental managers, operational staff, support staff (eg IT staff, security staff) as well as staff involved with information and information governance.

Where possible, we work with the person or organisation to schedule and agree interviews with them before the on-site visit. We give a schedule of areas we would cover, the information we require and discuss and agree the level and grade of staff we would interview (eg managers, operational staff).

We use questions to understand individual roles and processes they follow or manage, specifically referring to the handling of personal data and its security. Some questions may cover training and awareness, but they are not framed as a test, nor are they intended to catch people out.

We may conduct interviews at a person's desk or in a separate room, dependent upon circumstances and whether we need to observe the working environment or examine information and records. Interviews are normally 'one-to-one', but sometimes it may be appropriate to include several staff in an interview, for example, where they share responsibilities. ICO staff take notes or otherwise record the interviews.

Given the nature of interviews, we do not consider it necessary for third parties to accompany interviewees, but we would not object where someone reasonably requests a third party's participation.

We make every effort to restrict interviews to staff identified within the agreed schedule. But when it becomes clear that access to additional staff may be necessary, we would arrange this with the person or organisation's consent.

Interviews are to help us assess compliance. They do not form part of, or provide information for, any individual disciplinary or criminal investigation. Should evidence of a person's criminal activity emerge during an interview, we would halt the interview.

We may use people's names in distribution lists and the acknowledgements sections of full audit reports, but we would not reference them in the body of the reports or in any executive summary reports that we produce.

We may use job titles, where appropriate.

What happens when we finish our assessment?

In most cases, the outcome of the assessment is an audit report which we share with the person or organisation. The report sets out the information we considered as part of our assessment and how we reached our conclusions; it also includes recommendations to address any weaknesses or compliance issues that we identified. The organisation or person has the opportunity to review an initial draft of the report for the purpose of identifying any factual errors that may require addressing. For example, correcting department names or system names.

Following our assessment, we may decide that we do not need any further formal regulatory action. However, where we consider that we may need to take regulatory action, we may also share copies of the report internally. This would help us to decide what appropriate action (if any) we should take following the assessment. This could include formal enforcement action. Whatever we decide, we would communicate our decision to the person or organisation after we complete the assessment.

We publish executive summaries of our audit reports on our website. You can find full details about publication of our assessment notices in our policy on communicating our regulatory and enforcement activity.

Right of appeal

Under section 162 of the DPA 2018, recipients of assessment notices may appeal to the Tribunal. For the appeals procedure, please refer to The Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules.

Under section 164 of the DPA 2018, recipients of urgent assessment notices may apply to the court to disapply the statement of urgency or to change the time period for compliance.

Section 146(10) of the DPA 2018 allows us to cancel an information notice at any point. If we decide to cancel an assessment notice, we would provide written confirmation of this decision.

Further reading

More information about our memoranda and our agreements with other authorities is on our website: Working with other bodies

National security certificates The Information Commissioner is required to publish information about the existence of national security certificates.

Executive summaries of our audit reports are on our website: Action we've taken

The communicating regulatory and enforcement activity policy

Assessment notices DPA 2018 (Sections 146 - 147)

Destroying or falsifying information and documents (Section 148 DPA 2018)

A guide to ICO data protection audits

General Regulatory Chamber tribunal procedure rules - GOV.UK (www.gov.uk)

Enforcement notices

What is an enforcement notice?

An enforcement notice is a written notice we may issue to a person or organisation requiring them to take action to address any failings we identify in their data protection compliance. The notice may, for example, require the person or organisation to:

- improve their data security procedures;
- stop processing certain types of data; or
- provide training to staff.

We may issue enforcement notices in the circumstances set out in section 149 of the DPA 2018. For example, where a person or organisation breaches one of the data protection principles, or if a certification provider or monitoring body for a code of conduct is failing to meet their obligations.

The purpose of an enforcement notice is to either mandate action or to require the recipient to stop an ongoing or proposed action, such as data processing or transfer. This aims to either bring about compliance with the data protection legislation, remedy a breach or both. Failure to comply with an enforcement notice may result in us taking further action, including the possibility of issuing a penalty notice.

When would we issue an enforcement notice?

Enforcement notices are usually appropriate in cases that may require specific correcting or preventative action. When deciding whether to issue an enforcement notice, we consider:

- the likelihood of a person or organisation moving to compliance without compulsion;
- repeated failure to meet information rights obligations or their timescales (eg repeatedly delayed responses to subject access requests);
- evidence of a poor regulatory history;
- serious ongoing breaches of the rights and freedoms of the public;
- evidence of continued non-compliance during investigation or post-investigation;
- processing or transfer of information to a third country fails (or risks failing) to meet the requirements of the data protection legislation;
- a need for corrective action by a certification body or monitoring body to ensure that they meet their obligations; or
- the seriousness of risk or harm identified.

Before we issue a formal enforcement notice, we usually share the proposed content of the notice with the person or organisation concerned. This offers them the opportunity to comment on the notice and to provide us with any further information they think might affect our decision. We consider any information, including the provision of additional evidence, before reaching a final decision on enforcement action. In some cases, for example where we believe there is an actual or potential immediate risk to the public, we may issue an enforcement notice without prior consultation. All recipients of enforcement notices have a right of appeal.

How long do we normally give recipients to comply with an enforcement notice?

When we issue an enforcement notice, we give timescales for the recipient to complete the actions set out in the enforcement notice. Timescales may vary depending on the nature of the action we identified. For example, if a particular practice we identify during an investigation is causing serious harm to the public, we would require the person or organisation to stop immediately. Alternatively, if we wanted a person or organisation to retrain a large number of staff on appropriate data protection practices, or to procure new technological solutions, then we would allow a longer timescale to accommodate this. We require recipients of enforcement notices to provide evidence of their compliance within the required timescales.

When would we issue an urgent enforcement notice?

In addition, when deciding whether it is appropriate and proportionate to issue an enforcement notice with an urgency statement, and the timescale for compliance, we consider:

- the extent to which such urgent action may prevent or limit the risk of serious harm to the public or serious intrusion into their privacy. For example, requesting that an organisation or person stops using personal data for a specific purpose or takes action to protect personal data from security breaches;
- the nature and extent of work the enforcement notice requires; and
- the additional burden or impact on the recipient in having to comply with an urgent enforcement notice within the period we specify.

What does an enforcement notice contain?

The notice sets out:

- who is required to take the action and why;
- the specifics of the action to take;
- the timescales that apply for that action; and,

- any applicable appeal or challenge process.

What can we do if an organisation or person does not comply with an enforcement notice?

If a person or organisation does not comply with an enforcement notice, we would consider further action including, but not limited to, issuing a penalty notice (see below).

When deciding on further action we consider factors such as:

- how many of the actions set out in the enforcement notice are being complied with;
- what attempts the person or organisation made to comply;
- any ongoing risk to the public;
- the vulnerability of the people affected; and
- the person or organisation's compliance history.

Applications for cancellation or variation of an enforcement notice

Section 153(1) of the DPA 2018 allows us to cancel or vary an enforcement notice. If we decide to cancel or vary an enforcement notice, we would provide written confirmation of this decision.

A person to whom an enforcement notice is given may apply in writing to the Commissioner for the cancellation or variation of the notice (s153(2) DPA 2018). They may only make an application under section 153(2) DPA 2018:

- after the end of the period within which they can bring an appeal against the notice; and
- on the ground that, by reason of a change of circumstances, they do not need to comply with one or more of the provisions of that notice in order to remedy the failure the notice identifies.

A recipient of an enforcement notice may appeal to the Tribunal against the refusal of an application under section 153 DPA 2018 for the cancellation or variation of the notice (s162(2) DPA 2018).

Right of appeal

Under section 162 of the DPA 2018, recipients of enforcement notices may appeal to the Tribunal. For the appeals procedure please refer to The Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules.

Under section 164 of the DPA 2018, recipients of urgent enforcement notices may apply to the court to disapply the statement of urgency or to change the time period for compliance.

Further reading

Enforcement Notices DPA2018 (Sections 149 - 153)

General Regulatory Chamber tribunal procedure rules - GOV.UK (www.gov.uk)

Penalty notices

What is a penalty notice?

A penalty notice is a formal document that we issue (under section 155 DPA 2018) when we intend to fine a person or organisation for a breach, or breaches, of the data protection legislation we regulate. The penalty notice sets out the amount we intend to fine a person or organisation and the reasons for our decision.

Why do we issue penalty notices?

Our aim in applying penalty notices is to ensure compliance with legislation and information rights obligations. To do this, penalties must provide an appropriate sanction for any breach of data protection legislation, as well as an effective and proportionate deterrent to future non-compliance.

What is the process?

If we believe it may be necessary to issue a penalty notice, we would first issue a notice of intent (NoI). This explains why we believe a penalty notice is necessary and sets out details of the proposed penalty.

When a person or organisation receives an NoI, they can make representations to us about the content of the NoI and the proposed penalty. We carefully consider all representations before making a decision on whether to issue a penalty notice and, if so, what the penalty notice should include. We provide a detailed description of how we decide on appropriate penalties below.

When would a penalty notice be appropriate?

You should read this section alongside the "Regulatory responsibilities" section of the RAP. When deciding whether it is appropriate to impose a penalty notice, the Commissioner has regard to the considerations set out in section 155 of the DPA 2018.

We assess whether a penalty is appropriate in each individual case on the basis of the particular facts. To help us to consider the appropriateness of any potential penalty, we take into account a number of factors including:

Aggravating factors

- the attitude and conduct of the person or organisation concerned suggests an intentional, wilful or negligent approach to compliance or an unlawful business or operating model;
- the breach or potential breach is particularly serious (for example, whether it involves any critical national infrastructure or service. Critical national infrastructure includes buildings, networks and other necessary

systems that provide essential public services, for example energy, finance, telecoms and water services);

- a high degree of damage to the public (which may include distress or embarrassment);
- the data protection legislation breaches resulted in a relatively low degree of harm, but it affected many people;
- the person or organisation significantly or repeatedly failed to follow the good practice set out in the codes of practice we are required to promote;
- the person or organisation did not follow relevant advice, warnings, consultation feedback, conditions or guidance from us or the data protection officer (for data protection cases);
- the person or organisation failed to comply with an information notice, an assessment notice or an enforcement notice;
- the breach concerns novel or invasive technology;
- in data protection cases, if the person or organisation is certified by an accredited body under Article 43 of the UK GDPR, and failed to follow an approved or statutory code of conduct;
- the person or organisation's prior regulatory history, including the pattern, number and type of complaints about the issue and whether the issue raises new or repeated concerns that technological security measures are not protecting the personal data;
- the vulnerability, if any, of the affected people, due to their age, disability or other protected characteristic under the Equality Act 2010 (or section 75 Northern Ireland Act 1998);
- the breach involves special category data or a high level of privacy intrusion;
- the state and nature of any protective or preventative measures and technology available, including by design;
- the way we found out about the breach or issue and, if relevant, failure or delay by the person or organisation to notify us of the breach or issue; and
- if the person or organisation, directly or indirectly, gained any financial (including budgetary) benefits or avoided any financial losses.

Mitigating factors

- if the person or organisation notified us of the breach or issue early and has been open with us;
- any action the person or organisation took to mitigate or minimise any damage (including delay) that people suffered;
- any early action the organisation took to ensure future compliance with a relevant code of practice;

- in data protection cases, whether the person or organisation followed an approved or statutory code of conduct;
- the state and nature of any protective or preventative measures and technology available; and
- whether the person or organisation co-operated fully with us during any investigation.

Other factors we may consider

- the cost of measures to mitigate any risk, issue, or harm;
- the gravity and duration of a breach or potential breach;
- whether the person or organisation is representative of a sector or group, raising the possibility of similar issues arising again across that group or sector if they do not address them;
- any action the organisation took to report the breach to other appropriate bodies (such as the National Cyber Security Centre (NCSC)) and followed their advice;
- the public interest in taking regulatory action (for example, to provide an effective deterrent against future breaches or clarify or test an issue in dispute); and
- whether another regulator, law enforcement body or competent authority is already taking (or has already taken) action over the same matter.

What if an organisation or person does not agree with the content of an NoI?

As noted above, before issuing a penalty, we issue an NoI that advises the person or organisation that we intend to serve them with a penalty. The NoI sets out:

- their name and address;
- our investigative findings and the reasons why the Commissioner proposes to give a penalty notice; and
- the proposed level of penalty and any relevant aggravating or mitigating factors.

We invite written representations from the person or organisation about any aspect of the NoI. We allow the person or organisation at least 21 calendar days to make these representations. We consider these representations prior to our final determination as to whether a penalty is appropriate and, if it is appropriate, the level of penalty that we impose.

If we consider that it is appropriate for a person or organisation to make oral representations about our intention to give a penalty notice, then the NoI would state this. It would also specify the arrangements for making such

representations and the time at which, or period within which, they may make them.

If a person or organisation thinks that their circumstances warrant oral representations, they can explain how they justify this extra step in their written representations. In particular, we need to understand what oral representations would add to the information that an organisation has already provided in writing. We then decide whether or not to invite the organisation or person to a face-to-face meeting.

Where we are required to make reasonable adjustments under the Equality Act 2010, we would permit oral representations without the organisation or person making prior written representations.

We may convene a panel in cases where we are considering a fine in excess of £5m or in circumstances where we believe any proposed penalty or regulatory action is likely to cause a very significant financial impact on the recipient's business model.

The role of the panel is to decide whether the proposed fine (or any corrective measures) are effective, proportionate and dissuasive, by considering:

- the evidence in the case;
- the relevant legislation;
- the recommendations of the penalty setting meeting to the Commissioner;
- whether the action is consistent in scale and scope with our previous regulatory action; and
- any representations from organisations regarding the NoI.

The panel then makes a recommendation about the appropriate range of the fine or other corrective measures which they consider to be appropriate. They write a brief report which sets out the reasons for the panel's recommendation. The Commissioner has the final decision about the level of penalty we apply.

Schedule 16 of the DPA 2018 sets out full details of the information a penalty notice includes. We also advise those subject to penalties of any relevant rights of appeal.

How do we calculate the level of any penalty we impose?

We base our approach to the calculation of administrative penalties on the considerations set out in sections 155 to 157 of the DPA 2018.

The way we calculate financial penalties is fair, consistent and takes all relevant evidence and representations into account before we reach our final decision. We use a nine step process to help us to determine the level of any penalty, and we set this out in detail below.

The legislative caps

The law imposes clear upper limits for the level of any penalty. As set out in section 157(5)-157(6) of the DPA 2018, any penalty we impose cannot exceed the statutory maximum. The maximum amount (limit) of any penalty depends on the type of breach and whether the "standard maximum amount" (SMA) or "higher maximum amount" (HMA) applies, pursuant to s.157(2)-157(4) of the DPA 2018.

In the case of an undertaking, the standard maximum amount is £8,700,000 or 2% of turnover, whichever is higher. In any other case, the standard maximum amount is £8,700,000.

In the case of an undertaking, the higher maximum amount is £17,500,000 or 4% of turnover, whichever is higher. In any other case, the higher maximum amount is £17,500,000.

References to turnover in relation to penalty calculations is a reference to an undertaking's total annual worldwide turnover in the financial year which precedes the penalty calculation.

The level of penalty we impose within the above limits depends on the facts of the particular case. When determining the appropriate level, we ensure that the overall penalty sum is effective, proportionate and dissuasive. In determining this, we consider, in particular, the following factors:

- the nature, gravity and duration of the failure, taking into account the nature, scope or purpose of the processing concerned as well as the number of people affected and the level of damage they suffer;
- the intentional or negligent character of the failure;
- the degree of responsibility of the person or organisation in question, taking into account any technical or organisational measures they implemented;
- the organisation's turnover (in the event that they are undertakings) or the economic situation of any other person that we would impose a fine;
- any relevant previous failures by the person or organisation;
- the degree of co-operation with us in order to remedy the failure or mitigate its effects;
- the categories of personal data that the failure affected;
- whether the person or organisation notified us of the failure;
- the person or organisation's previous history of compliance with notices we issued;
- adherence to approved codes of conduct or approved certification mechanisms;
- any other aggravating or mitigating factors or, where applicable, both;

and

- any sufficiently similar or relevant previous decisions by us and other data protection regulators.

Having calculated the penalty sum on the basis of these factors, we also consider the wider economic impact of imposing the penalty sum. We also apply any reductions for early payment (see below).

An appropriate person within the ICO determines the final decision on the amount of an administrative. Our scheme of delegations explains the decision-making powers our staff hold and which staff have the authority to make decisions regarding administrative penalties. You can find the scheme of delegations on our website.

The nine steps before making a recommendation on a penalty amount

For each case, we complete the following nine steps before we make our recommendation on the amount of an administrative penalty:

Step one	Assessment of seriousness considering relevant factors under section 155 DPA 2018.
Step two	Assessment of whether the failure was intentional or due to negligence.
Step three	Determination of turnover or equivalent (where applicable).
Step four	Calculation of an appropriate starting range.
Step five	Consideration of other relevant aggravating and mitigating features.
Step six	Consideration of ability to pay.
Step seven	Assessment of economic impact.
Step eight	Assessment of effectiveness, proportionality and dissuasiveness.
Step nine	Early payment reduction.

The considerations at each step are:

Step one: Assessment of seriousness considering relevant factors under

section 155 DPA 2018

We start by considering the seriousness of the failure. We do this by taking into account sections 155 (3) (a), (c), (d), (e), (f), (g), (h), (i) and (j) of the DPA 2018 and Article 83(2) UK GDPR, specifically:

- the nature, gravity and duration of the failure, taking into account the nature, scope or purpose of the processing concerned as well as the number of people affected and the level of damage they suffered;
- any action the person or organisation took to mitigate the damage suffered by people;
- the degree of responsibility of the person or organisation, taking into account technical and organisational measures implemented by them in accordance with section 56, 66, 103 or 107; any relevant previous failures by the organisation or person;
- the degree of co-operation with us, in order to remedy the failure and mitigate the possible adverse effects of the failure;
- the categories of personal data that the failure affected;
- the way we found out about the breach, including whether, and if so to what extent, the person or organisation notified us of the failure;
- the extent to which the person or organisation complied with previous enforcement notices or penalty notices; and
- their adherence to approved codes of conduct or approved certification mechanisms.

We assess seriousness on a scale using levels of low, medium, high and very high. Possible examples for each level are as follows:

"low" seriousness:

- A minor infringement, short in duration with a low number of impacted people and where the affected data did not contain special category data or where people did not suffer any damage. The person or organisation fully complied with reporting requirements and has no relevant regulatory history.

"medium" seriousness:

- A moderate level infringement, short in duration with a limited number of affected people or where there is limited damage to members of the public. The person or organisation partially complied with reporting requirements and has no or little relevant regulatory history.

"high" seriousness:

- A serious infringement which occurred over a prolonged time period, with a high number of people affected or significant damage to the

public involving, for example, special category data. The person or organisation reported the incident late and has some relevant regulatory history.

"very high" seriousness:

- A very serious infringement which occurred over a prolonged time period with a very high number of people affected or significant damage to the public involving, for example, special category data. The person or organisation failed to report the incident and has significant relevant regulatory history.

The above examples are general indicators only, and we will take into account all the relevant Article 83 considerations when making a decision as to seriousness.

Step two: Assessment of whether the failure was intentional or due to negligence

In accordance with section 155 (3) (b) DPA 2018 and Article 83 (b) UK GDPR, we also take into account the intentional or negligent character of the failure. This looks at specifically whether the person or organisation was intentional or negligent about their responsibility for the failure.

Intention involves knowledge and wilfulness. Examples of intentional failures might be unlawful processing authorised explicitly by the organisation's top management hierarchy, or in ignoring their DPO's advice.

We consider negligent failures to be those which are unintentional. This is where the person or organisation did not intend to cause the failure, but nevertheless they failed to comply with data protection law. Examples of negligent failures may be failure to:

- check for personal data in published information; or
- read and follow existing policies.

Step three: Determination of turnover or equivalent

Article 83(4)-83(5) UK GDPR and section 157 of DPA 2018 set out the maximum amount of a penalty that we may impose on an undertaking with reference to turnover. We also use turnover or equivalent to determine the starting range for a penalty (see step four) for undertakings and non-undertakings, to provide consistency and fairness in penalty setting.

To establish turnover or equivalent, we review the relevant financial information and obtain expert financial or accountancy advice if we require. Where necessary, we will ask for financial information to help us to understand the circumstances. Where there is a lack of co-operation in

providing all relevant financial information, the panel may decide to rely on the information that is available, or otherwise give greater weight to the factors they consider in other steps of the process (such as aggravating features under step five).

Where the subject of a penalty is not commercial in nature and may not therefore have a turnover, we will consider equivalent information on the relevant financial circumstances, including income, budgets or expenditure.

We consider turnover to be a relevant consideration when settling upon a penalty amount which is dissuasive and proportionate, however it is not determinative. In certain circumstances, in order to be sufficiently dissuasive, we may need to set a relatively high penalty even where an undertaking has a comparatively low turnover, or no history of turnover.

We will determine the relevant undertaking by taking into account the circumstances of every case. We will primarily review the ownership structures of the entities involved to determine which form part of the undertaking. It may be that, for example, the data controller or processor is a subsidiary of a parent company and together they constitute a single economic unit and single undertaking. In those circumstances, where there is sufficient evidence, we will calculate the penalty with reference to the turnover of the undertaking as a whole rather than the turnover of the controller or processor concerned.

Step four: Calculation of an appropriate starting range

We determine a starting range for the calculation of the penalty as set out below. We base the starting range for the penalty on the seriousness of the breach, as evaluated at step one above. We will then apply the appropriate percentage to the turnover or equivalent as determined at step three. The starting point will be determined by taking into consideration the assessment of whether the failure was intentional or due to negligence, as determined at step two.

For infringements where the standard maximum amount (SMA) applies, we consider the following starting ranges to be appropriate:

- For infringements with a low-level of seriousness, an appropriate starting range would be 0-0.5% of turnover or equivalent.
- For infringements with a medium-level of seriousness, 0.5-1% is an appropriate starting range.
- For infringements of a high-level of seriousness, 1-1.5% is an appropriate starting range.
- For infringements of a very high-level of seriousness, 1.5-2% is an

appropriate starting range.

In determining a starting point within that range, we consider whether the failure was intentional or due to negligence in the specific circumstances of the case. Those who have acted negligently can expect a lower starting point than those who have acted intentionally.

For infringements where the higher maximum amount (HMA) applies, we consider the following starting ranges to be appropriate:

- For infringements with a low-level of seriousness, an appropriate starting range would be 0-1% of turnover or equivalent.
- For infringements with a medium-level of seriousness, 1-2% is an appropriate starting range.
- For infringements of a high-level of seriousness, 2-3% is an appropriate starting range.
- For infringements of a very high-level of seriousness, 3-4% is an appropriate starting range.

In determining a starting point within that range, we consider whether the failure was intentional or due to negligence in the specific circumstances of the case. Those who have acted negligently can expect a lower starting point than those who have acted intentionally.

In determining the starting point of the penalty, we will use rounded figures.

Step five: Consideration of other relevant aggravating and mitigating features

In line with section 155 (3) (k) DPA 2018 and Article 83 (2) (k) UK GDPR, we consider any aggravating or mitigating factors which we have not already considered in previous steps. These include, where applicable, factors such as any financial benefits the organisation or person gained, or losses avoided from the breach (whether directly or indirectly).

When determining the amount of any proposed administrative fine, we adjust the starting point figure for each band accordingly, upwards or downwards, to reflect our considerations of the above. We clearly record which aggravating and mitigating features we take into account and why and how we consider that these features influence the proposed administrative penalty.

Step six: Consideration of ability to pay

Based on the information available, we consider the likelihood of the proposed recipient of the penalty being able to pay the proposed penalty and whether it may cause undue financial hardship. If required, we review or obtain expert financial or accountancy advice in support of this step.

This is particularly important if an organisation or person's ability to pay is unclear or they have had a recent change in their financial, trading or competitive status. We would ask the organisation or person for information about their ability to pay, as appropriate.

Should a claim of financial hardship be made, we will expect it to be supported by evidence including (but not limited to) historical financial statements and other information considered relevant, such as internal forecasts.

Step seven: Assessment of economic impact

We must consider the desirability of promoting economic growth when exercising our regulatory functions under the DPA 2018, in accordance with our duties under section 108 of the Deregulation Act 2015. As such, we must ensure that we only take regulatory action when we need to, and that any action we take is proportionate. We must take this into consideration whenever we exercise a specified regulatory function.

We therefore consider the impact of any proposed penalty on economic growth, both in terms of the impact on the intended recipient, and more broadly.

We may consider agreeing payment of monetary penalties in instalments. This would depend on the recipient showing, to our satisfaction, that there are economic, financial or other reasons, why this is necessary.

We would not make any agreement to allow payment in instalments where the payment would no longer be effective and dissuasive.

Step eight: Assessment of effectiveness, proportionality and dissuasiveness

We ensure that the amount of the fine we propose is effective, proportionate and dissuasive. We can adjust it accordingly, in line with section 155 (3) (l) DPA 2018 and Article 83 (1) UK GDPR.

We also confirm that the final level of penalty imposed complies with the applicable cap (as set out in the section above on legislative caps).

Where there are multiple linked infringements, we shall consider them together and calculate a total penalty which shall not exceed the applicable cap for the gravest infringement.

Step nine: Early payment reduction

We would reduce the monetary penalty by 20% if we receive full payment within 28 calendar days of sending the notice. This early payment reduction does not apply in circumstances where we agreed an instalment plan.

Applications for cancellation or variation of a penalty notice

We may vary a penalty notice by giving written notice (a "penalty variation notice") to the person or organisation in question (Schedule 16, 7(1) DPA 2018).

We may cancel a penalty notice by giving written notice to the person or organisation in question (Schedule 16, 8(1) DPA 2018).

Right of appeal

Under section 162 of the DPA 2018, recipients of penalty notices may appeal to the Tribunal. A recipient of a penalty notice or a penalty variation notice may appeal to the Tribunal against the penalty amount, whether or not the person or organisation appeals against the notice (s162(3) DPA 2018). For the appeals procedure, please refer to the Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules.

Further reading

Penalty notices DPA 2018 (sections 155-159)

Schedule 16 DPA 2018

Deregulation Act 2015

Scheme of delegations

General Regulatory Chamber tribunal procedure rules - GOV.UK (www.gov.uk)

Fixed penalties

Section 137 of the DPA 2018 states that persons or organisations who are data controllers must pay a registration fee to the ICO. The further reading section below has more information on fees and how to pay them.

Section 158 of the DPA 2018 provides information on the fixed penalty notices we can issue for failing to meet specific obligations. For example, we can issue a penalty notice for failing to pay the relevant fee to us. Where those provisions apply, we levy penalties in accordance with the law. The fixed penalty payable by an organisation or person for failing to pay a data protection fee in accordance with the Data Protection (Charges and Information) Regulations 2018, is:

- tier 1 (micro-organisations) £400;
- tier 2 (small and medium organisations) £600; or
- tier 3 (large organisations) £4,000.

Further reading

You can find out more about how to register as a data controller and associated fees: Data protection fee

Fixed Penalties DPA 2018 (Section 158)

Privileged communications

Section 133(5) of the DPA 2018 defines privileged communications. Under this section, we must publish guidance about how we ensure that we only use or disclose any privileged communications, which we obtain or have access to, so far as is necessary to carry out our functions. We also need to publish guidance about how we comply with restrictions or prohibitions relating to obtaining or accessing privileged communications.

Sections 143(3)-143(4) and 147(2)-147(3) of the DPA 2018 say that an information or assessment notice's requirement to provide or disclose information does not apply to any privileged communications about data protection legislation.

We would not seek to obtain or access any legally privileged material, whether this relates to data protection legislation or not.

In circumstances where we are informed or have reasonable grounds to suspect that any of the disclosed, obtained or seized data contains legally privileged material, we would follow a process to ensure that we extract, return and do not rely on such material. The process takes into account the Attorney General's Guidelines on Disclosure 2020 in respect of legal professional privilege.

The process would involve, if required, the instruction of independent counsel to review the material to determine the issue of legal privilege (taking into account the Bar Council's Guide to Independent Counsel 2010).

In relation to digital material, the process would also involve, if required, the instruction of an independent forensic consultant to search for and isolate any potentially legally privileged material for review by independent counsel as above.

A privilege holder may wish, for their own purposes, to waive privilege in legally privileged material that we obtain or is provided to us; this is their choice. However, should they choose to do so, we cannot accept any condition to that waiver which would restrict our ability to use that material in the exercise of our statutory functions. Therefore, we can only accept a full and unconditional waiver of privilege. If that is not acceptable to a privilege holder, they should not provide to us any legally privileged material.

In any event we do have a duty of confidentiality under section 132 of the DPA 2018. Unless we make the disclosure with lawful authority, we must not disclose information which:

- we obtain or is provided to us in the course of, or for the purposes of, the discharging of our functions;
- relates to an identified or identifiable person or business; and
- is not available to the public from other sources at the time of the

disclosure and was not previously available to the public from other sources.

Section 132(2) of the DPA 2018 sets out the circumstances when disclosure would be made with lawful authority; for example, if we make the disclosure for the purposes of, and is necessary for, the discharge of our functions.

Further reading

Guidance about privileged communications DPA 2018 (Section 133)

Bar Council's Guide to Independent Counsel 2010

Attorney General's Guidelines on Disclosure 2020

Attorney General's Guidelines on Disclosure 2020 pdf

Effectiveness of regulatory action

Our strategic plan sets out the measures we use to assess the effectiveness of our work.

We report annually to Parliament about our work, including our regulatory activity and, where needed, our formal enforcement actions. This may also include reporting on specific issues with individual organisations, sectors or public authorities, where we identified and addressed systemic information rights problems.

> **Further reading**
>
> Strategic plan [this document will be updated in due course]

Evaluation and next steps

We will keep this guidance under review and will update it, as and when necessary, to reflect any amendments to the legislation which this guidance covers.