Statutory guidance on our regulatory action

ico.
Information Commissioner's Office

Contents

Foreword

A foreword will be inserted 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 the Regulatory action policy. Taken together those documents set out how the ICO will support this mission. This Statutory guidance focuses on our data protection obligations and details how the ICO will exercise its regulatory functions when issuing information notices, assessment notices, enforcement notices and penalty notices.

The purpose of this document is to provide clarity to those we regulate and the public about our chosen approach to statutory regulatory action. This will help the ICO achieve the goals we set out in our Information rights strategic plan.

This document sets out our risk-based approach to taking regulatory action against organisations and individuals that have breached the provisions of data protection law, set out in our aims below. Our focus is on the areas of highest risk and most harm and the principles we apply in exercising our powers.

The ICO's approach is designed to help create an environment within which, data subjects are protected, while ensuring business is able to operate and innovate efficiently in the digital age. We will be as robust as we need to in upholding the law, whilst ensuring that commercial enterprise is not constrained by red tape or concern that sanctions will be used disproportionately. We will work with others where it makes sense to do so, and where joint application of activity can achieve the best result and protection.

To maintain an effective and proportionate regulatory response, this guidance seeks to:

- set out the nature of the ICO's 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 individuals' information rights are properly protected; and
- assist delivery of the goals set out in our Information rights strategic plan and uphold information rights effectively for individuals in the digital age.

In addition, by issuing this document we are:

- fulfilling our statutory obligation to provide guidance as to how we propose to exercise our functions in connection with information notices, assessment notices, enforcement notices, and penalty notices (See section 160(1) DPA 2018).

- providing guidance (section 133(1)(a) DPA 2018) as to how we propose to secure that privileged communications which we obtain or have access to in the course of carrying out our functions are used or disclosed only so far as necessary for carrying out those functions, and (section 133(1)(b) to provide guidance in how we propose to comply with restrictions and prohibitions on obtaining or having access to privileged communications which are imposed by an enactment; and
- fulfilling our statutory obligation (See section 158 DPA 2018) to produce and publish a document specifying the amount of the penalty for a failure to pay the data protection fees required under section 137 of the DPA 2018.

This document contains all guidance on the ICO's approach to the use of our regulatory powers that we have a statutory obligation to provide under the Data Protection Act 2018 (DPA 2018). The full range of our other regulatory activity and other law we regulate is set out in our Regulatory action policy (this is available on our website and is currently under review).

Who is this guidance for?

This guidance is to inform data controllers, processers and the public about the statutory powers the ICO can use to investigate and enforce data protection legislation in the UK.

It explains how we decide to use our powers and how we make decisions about our enforcement action, including how we calculate financial penalties.

What is the status of this guidance?

The ICO is required by law to produce guidance on how we use our statutory powers. In producing this document, we have consulted ICO colleagues, we will run a formal consultation with the public and finally lay this guidance before Parliament for approval. We will keep this guidance under review to ensure it remains relevant and accurate.

We are empowered to take various regulatory actions for breaches of the following legislation:

- Data Protection Act 2018 (DPA 2018); and
- General Data Protection Regulation (GDPR: Regulation (EU)2016/679) (GDPR).

> **Further reading**
>
> Information Rights Strategic Plan (IRSP)

> 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) (this document is currently under review).

Regulatory activity covered by this guidance

Our regulatory activity includes:

- conducting assessments of compliance with the DPA 2018 and GDPR (which we refer to in this document as the 'data protection law');
- issuing information notices;
- issuing 'urgent' information notices under the DPA 2018, requiring individuals, data controllers or processors to provide information on not less than 24 hours' notice;
- applying for a court order requiring compliance with the information notice issued under the DPA 2018, if the recipient does not provide a full and timely response;
- issuing assessment notices under DPA 2018;
- issuing 'urgent' assessment notices under the DPA 2018, requiring data controllers or processors to allow us to undertake an assessment of whether they are compliant with data protection law, on not less than seven days' notice;
- issuing no-notice (or short notice) assessment notices under the DPA 2018 where we have reasonable grounds to suspect that the data controller or processor has:
    - failed or is failing to comply with certain provisions of the data protection legislation (set out in section 149(2) DPA 2018); or
    - has committed or is committing an offence under the DPA 2018, allowing us to undertake an assessment on less than seven days' notice;
- issuing enforcement notices requiring specific actions by an individual or organisation to resolve breaches (including breaches) of applicable information rights obligations. An 'urgent' enforcement notice under the DPA may be used to require action to resolve breaches or potential breaches of the data protection law, on not less than 24 hours' notice;
- administering fines by penalty notices in the circumstances set out in section 155 of the DPA 2018;
- administering fixed penalties for failing to meet specific obligations (a failure to pay the relevant fee to the ICO); and

- prosecuting criminal offences before the courts.

We provide a suite of guidance to organisations and individuals about how to comply with the law and support this with advice. This can take the form of letters of advice, compliance meetings, presentations, conferences, and advice sessions, in addition to advice provided via our helpline, live chat and on our website.

The full range of our enforcement powers, together with the regulatory actions associated with these powers, and the legislation we regulate, are set out on our website.

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

Information notices

What is an information notice?

An information notice is a formal request (under section 142 of the DPA 2018) for a data controller, processor or individual to provide the ICO with information, within a specified time frame, to assist us with our investigations. We will issue an information notice when we consider it necessary to do so. In some circumstances it may be a criminal offence to provide a response which is false.

When will we issue an information notice?

We will serve an information notice at our discretion. We will consider what action is appropriate and proportionate, including:

- the risk of harm to individuals or the level of intrusion into their privacy potentially posed by the events or data processing under investigation;
- the necessity of requiring a formal response within a defined time period;
- the necessity of testing responses, by the fact that it is an offence to deliberately or recklessly make a false statement in a material respect in response; and
- the public interest in the response.

When deciding the period for compliance with information notices and whether to issue an 'urgent' information notice, we will consider what action is appropriate and proportionate, including:

- the extent to which urgent investigation may prevent or limit the risk of serious harm to individuals or serious intrusion into their privacy;
- the extent to which urgent investigation may prevent the alteration, destruction, concealment, blocking, falsifying, or removal of relevant evidence of data processing;
- the scope of the notice, that is the scope of questions or requests in an information notice;
- the additional burden on the recipient in having to comply with a notice urgently;
- the impact on the rights of the recipient should we gain access to its premises and data processing activities urgently, without notice or on short notice, and without the opportunity to appeal or for an appeal to be heard by the Information Tribunal or both;
- the length of time of the investigation. For example, it may be appropriate and proportionate to issue an urgent information notice during a long running investigation where the questions are limited, and the response may bring the investigation closer to completion; and
- the comparative effectiveness of other investigatory powers of the ICO.

What action will we take if an organisation does not respond to an information notice on time?

If a recipient of an information notice does not fully respond within the applicable time, whether urgent or not, we may promptly apply for a court order requiring a response. We may decide not to make an application, having considered certain criteria, including:

- the reasons for non-compliance with the information notice;
- any commitments given by the recipient to responding to the information notice;
- whether the information has been or is likely to be obtained from another source;
- the comparative effectiveness of other investigatory and enforcement powers of the ICO. For example, we may decide we have sufficient evidence to move to an enforcement action in any event; and
- the public interest.

We will also consider whether to issue a penalty notice (see below).

Further reading

Information Notices DPA2018 (Sections 142 - 145)

Destroying or falsifying information and documents (Section 148 DPA2018)

Assessment notices

What is an assessment notice?

The DPA 2018 (section 146) contains a provision for the ICO to issue an assessment notice. This is, essentially, a notice we issue to a data controller or processor to allow us to consider whether they are compliant with data protection legislation. The notice may, for example, require the data controller or processor to give us access to premises and specified documentation and equipment. In some circumstances it may be a criminal offence to provide a response which is false.

When will we issue an assessment notice?

We may serve an assessment notice at our discretion as part of our consideration about whether an organisation is complying with data protection legislation. We will consider what action is appropriate and proportionate, including whether:

- our risk assessment process, or other supervisory and regulatory activity, indicates that the organisation is not complying with data protection legislation when processing personal data, together with a likelihood of damage or distress to individuals;
- it is necessary to verify compliance with an enforcement notice;
- communications with or information (eg news reports, statutory reporting, or publications) about the data controller or processor suggest that they are not complying with data protection legislation when processing personal data; and
- the data controller or processor has failed to respond to an information notice within an appropriate time.

When deciding the period for compliance with assessment notices, in particular whether to issue an 'urgent', 'no-notice' or 'short-notice' assessment notice, we will consider what action is appropriate and proportionate, including:

- the extent to which urgent investigation may prevent or limit the risk of serious harm to individuals 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 the notice, that is the scope of our requests in an assessment notice;
- the additional burden on the recipient in having to comply with a notice urgently, on no-notice or on short-notice;
- the impact on the rights of the recipient should we gain access to its premises and data processing activities urgently, without notice or on short notice, and without the opportunity to appeal or for an appeal to be heard by the Information Tribunal or both;
- the length of time of the investigation. For example, it may be appropriate and proportionate to issue an urgent assessment notice during a long running investigation where the requests are limited, and the response may bring the investigation closer to completion; and
- the comparative effectiveness of other investigatory powers of the ICO.

What action will we take if an organisation fails to respond to an assessment notice?

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

If a data controller or processor fails to comply with an assessment notice, we will consider whether to issue a penalty notice (see below).

What about assessments of documents, including the handling of health and social care records?

We may require access to the specified documents and information, or classes of documents and information, which define and explain how an organisation has met its obligations under the legislation, and what governance controls it has in place to measure compliance.

Although not an exhaustive list this 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; and
- job descriptions.

We may also need access to specified personal data or classes of personal data, and to evidence that the organisation is following the policies and procedures which ensure compliance with the legislation. We will access the minimum amount of information we need to assess whether the organisation is handling personal data appropriately.

We may require access to information which:

- is subject to legal professional privilege – where this information does not relate to data protection law (see section on privileged communications below);
- has a high level of commercial sensitivity;
- is exempt information as defined by section 23 of the Freedom of Information Act 2000 (information supplied by, or relating to bodies dealing with security matters); or
- is exempt from the DPA 2018, by virtue of a national security certificate.

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 possible, we will try and assess compliance without looking at this type of information. Where it is necessary and appropriate, we will ensure that properly vetted members of staff inspect such sensitive information. We have memoranda of understanding with relevant agencies to provide access and explanation of this type of material.

Organisations can contact us to request that, if an assessment notice requires access to such information, this access is limited to the minimum required to adequately assess their compliance with the legislation. They may also request other access conditions. We will try to accommodate such requests if we are satisfied that doing so would not compromise the effectiveness of our assessment. An organisation must make these requests within 28 days of the notice, unless the assessment is to be conducted on shorter notice, in which case, as soon as reasonably possible.

We may need to view health and social care records. If we do, we will respect the confidentiality of this data, and will limit access to the minimum required to adequately assess compliance. We will not take the content of these off-site, neither will we copy or transcribe them into working notes, and we will not include them in any reporting of the assessment.

What about inspection and examinations during assessments?

Inspections and examinations are key review elements of our assessment. They help us to identify objective evidence of how an organisation is complying and implementing policies and procedures.

We use these reviews to evaluate how an organisation:

- obtains, stores, organises, adapts, alters information or personal data;
- ensures the confidentiality, integrity and availability of the data or service it provides;
- retrieves, consults, or uses the information or personal data;
- discloses personal data by transmitting or disseminating or otherwise making the data available; and
- weeds and destroys personal data.

In our review of personal data, and associated logs and audit trails, we may consider:

- both manually and electronically stored data, including data stored centrally, locally and on mobile devices and media;
- management/ control information, to monitor and record how a data controller is processing personal data and meeting their wider obligations under the legislation; and
- physical and IT-related security measures, including how a data controller 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 information is held electronically, we may require the data controller 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.

We would only take data reviewed as part of the review and evaluation process, but not specifically identified in the assessment notice, off the data controller's site with their permission.

What about interviews carried out during assessments?

Interviews will consist of discussions with:

- staff and contractors;
- any processor's staff; and
- staff of relevant service providers as specified in the assessment notice.

We conduct interviews to develop further understanding of working practices or awareness of regulatory obligations or both. We may interview departmental managers, operational staff, support staff (eg IT staff, security staff) as well as staff involved with information and information governance.

Where possible we will schedule and agree interviews with the data controller or processor before the on-site visit. We will give a schedule of areas to be covered and will discuss and agree the level and grade of staff to be interviewed (eg managers, operational staff etc). The organisations should advise individuals in advance that they are required to participate.

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

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

Given the nature of interviews we do not consider it necessary for interviewees to be accompanied by third parties, but we will not object where it is reasonably requested.

We will 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 will arrange this with the consent of the data controller. Similarly, the schedule will not prevent us having confirmatory conversations with a consenting third party, for example where the third party is close to a desk-side discussion.

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 criminal activity by an individual emerge during an interview, we will halt the interview.

We may use individuals' names in distribution lists and the acknowledgements sections of reports, but we will not reference them in the body of any report.

We may use job titles, where appropriate.

What happens when we finish our assessment?

In most cases the outcome of the assessment will be an audit report which we will share with the organisation. The report will set out the information we considered as part of our assessment and how we reached our conclusions; it will also include recommendations to address any weaknesses or compliance issues that are identified. Following our assessment, we may decide no further formal action is needed. However, we may also share copies of the report internally to help us to decide what action (if any) the ICO should take following the assessment – this could include formal enforcement action. Whatever we decide, we will communicate our decision to the organisation after the assessment is complete.

We publish executive summaries of our audit reports on our website. Full details about publication of our assessment notices can be found in our Communicating our Regulatory and Enforcement Activity Policy.

Further reading

More information about our memorandums and what agreements we have 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 the ICO website: Action we've taken

CREAP The Communicating Regulatory and Enforcement Activity Policy.

Assessment Notices DPA2018 (Sections 146 - 147)

Destroying or falsifying information and documents (Section 148 DPA2018)

Enforcement notices

What is an enforcement notice?

The ICO may issue enforcement notices in the circumstances set out in section 149 of the DPA 2018. For example, where a data controller or processor has breached 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 mandate action (or halt action, such as processing or transfer) to bring about compliance with information rights or remedy a breach or both. Failure to comply with an enforcement notice invites further action, including the possibility that we may issue a penalty notice.

When will we issue an enforcement notice?

Enforcement notices will usually be appropriate where specific correcting action (or its prevention) may be required, for example:

- repeated failure to meet information rights obligations or timescales for them (e.g. repeatedly delayed subject access requests);
- serious ongoing infringements to the rights and freedoms of individuals;
- processing or transfer of information to a third country fails (or risks failing) to meet the requirements of the data protection legislation; or
- a need for correcting action by a certification body or monitoring body to ensure that they meet their obligations.

The notice will set out:

- who is required to take the action and why;
- the specifics of the action to be taken;
- the timescales that apply for that action; and,
- any appeal/ challenge process that applies.

When deciding whether to issue an enforcement notice, we will consider the factors set out above, including whether there are any mitigating or aggravating factors.

On occasions where we consider it to be appropriate, we may provide a preliminary version of the enforcement notice we intend to serve. This allows the recipient to comment on it and provide us with any further information they think might affect our decision to issue an enforcement notice.

Timescales set out in an enforcement notice will usually reflect the:

- imminence of proposed action that could lead to a breach of obligations;
- severity and scale of any breach/ failings; and
- feasibility (including lead times) of any correcting measures or technology.

In addition, when deciding whether it is appropriate and proportionate to issue an 'urgent' enforcement notice, and the timescale for compliance, we will consider:

- the extent to which such urgent action may prevent or limit the risk of serious harm to individuals or serious intrusion into their privacy. For example, requesting a data controller stops using personal data for a

specific purpose or takes action to protect personal data from security breaches;

- the scope of the enforcement notice;
- the additional burden or impact on the recipient in having to comply with an urgent enforcement notice within the period specified; and
- the comparative effectiveness of other enforcement powers of the ICO.

What will we do if an organisation does not comply with an enforcement notice?

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

> **Further reading**
>
> Enforcement Notices DPA2018 (Sections 149 - 153)

Penalty notices

What is a penalty notice?

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

Why do we issue penalty notices?

Our aim in applying penalty notices is to punish an organisation for breaches of data protection law and to promote future compliance with the law and information rights obligations. To do this, penalties must provide an appropriate sanction for any breach of data protection law, as well as act as an effective deterrent.

When will a penalty notice be appropriate?

In most cases we will reserve our powers for the most serious breaches of information rights obligations. These will typically involve intentional or negligent acts, or repeated breaches of information rights obligations, causing damage to individuals. In considering the degree of damage we may consider that, where there is a lower level of impact across many individuals, the totality of that damage may be substantial and may require a sanction. We can serve penalty notices on both data controllers and processors.

We will assess each case objectively based on the facts. But our risk-based approach means that it is more likely that we will impose a penalty where, for example:

- many individuals have been affected;
- the breaches concern processing which is unlawful, unfair, or which is not transparent;
- there has been a degree of damage (which may include distress and/or embarrassment);
- special category data has been involved;
- there has been a failure to comply with an information notice, an assessment notice, or an enforcement notice;
- there has been a repeated breach of obligations or a failure to rectify a previously identified problem or follow previous recommendations;
- intentional action (including inaction) is a feature of the case;
- there has been a failure to apply reasonable measures to mitigate any breach (or the possibility of it); and
- the data controller or processor is highly culpable for the breach.

What if an organisation does not agree with the content of a penalty notice?

Before issuing a penalty, we will issue a notice of intent (NOI) that will advise the organisation or individual that we intend to serve them with a penalty. The NOI sets out:

- the circumstances of the breach;
- our investigative findings;
- the proposed level of penalty;
- a rationale for the basis; and
- the amount of the penalty.

If an organisation disagrees with the content of our NOI then they can contact us.

We will invite written representations from the organisation or individual about the imposition of the penalty and its proposed amount. The organisation or person will be allowed at least 21 calendar days to make these representations. We will consider these representations prior to our final determination as to whether a penalty is appropriate.

In addition, we may allow an organisation or individual subject to an NOI to submit representations verbally. However, this is discretionary and only relevant

in cases that are considered by us to be exceptional. It is likely that these could be appropriate in circumstances where:

- the central facts of any breach or failing are in dispute; or
- there is a requirement to make reasonable adjustments under the Equality Act 2010.

During these meetings, representatives of the organisation or individual issued with the NOI are able to explain in person:

- how the privacy concerns and breach(es) occurred;
- whether there are any mitigating factors;
- what they have (or plan to do) to achieve compliance; and
- why they believe that the ICO should not take the intended regulatory action.

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

However, it is unlikely that we will agree to take oral representations in a case that is principally technical in nature. In such cases, it is normally more appropriate to consider complex technical representations in writing.

When applicable, we will also consider representations (including from any other Concerned Supervisory Authorities) in setting the final amount of any penalty. These representations will be taken after we have received any feedback from the intended recipient of the penalty but before we set the final penalty level.

For significant penalties a panel comprising non-executive advisors to the ICO may be convened by the Commissioner. They will consider the investigation findings and any representations made, before making a recommendation to the Commissioner about any penalty level to be applied. It will be the Commissioner's final decision about the level of penalty applied. The panel may comprise technical experts in areas relevant to the case under consideration.

Once all representations have been fully considered, we will confirm any penalty notice in writing. Full details of the information included in a penalty notice are set out in schedule 16 of the DPA 2018. We will also advise those subject to penalties of any relevant rights of appeal.

What will be the amount of any penalty?

This is our approach to the calculation of administrative penalties under sections 155 to 157 of the DPA 2018 and Article 83 of the GDPR.

The maximum amount (limit) of any penalty depends on the type of breach and whether the 'standard maximum amount' or 'higher maximum amount' applies. The higher maximum amount is, in the case of an undertaking, 20 million Euros or 4% of turnover, whichever is higher, or in any other case, 20 million Euros. The standard maximum amount is, in the case of an undertaking, 10 million Euros or 2% of turnover, whichever is higher, or in any other case, 10 million Euros.

Where a fine based on turnover exceeds the 10 or 20 million Euros limit, we will cap the fine at the relevant limit. We may impose a fine up to the relevant limit, if a fine based on turnover would not result in a proportionate fine because, for example, a company has a very low or no turnover (but has committed a serious breach of data protection law).

Where we have discretion to set the amount of any penalty in the context of our regulatory work, we will base this on the nine-step mechanism described below, within the legislative limits.

We will calculate the recommended amount of a proposed administrative penalty, based on:

- the seriousness of the contravention;
- the degree of culpability of the organisation concerned;
- our determination about turnover;
- any aggravating or mitigating factors or both;
- the means of the organisation to pay;
- the economic impact;
- the effectiveness, proportionality and dissuasiveness of any penalty; and finally
- any early payment reduction.

The final decision on the amount of an administrative penalty is determined by an appropriate person within the ICO.

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

Step 1	Assessment of seriousness considering relevant factors under section 155 DPA 2018
Step 2	Assessment of degree of culpability of the organisation concerned
Step 3	Determination of turnover

Step 4	Calculation of an appropriate starting point
Step 5	Consideration of relevant aggravating and mitigating features
Step 6	Consideration of financial means
Step 7	Assessment of economic impact
Step 8	Assessment of effectiveness, proportionality and dissuasiveness
Step 9	Early payment reduction

The considerations at each step are:

Step 1: Assessment of seriousness considering relevant factors under section 155 DPA 2018

Firstly, we will decide whether the higher maximum amount (4% of relevant turnover or 20 Million Euro) or the standard maximum amount (2% of relevant turnover or 10 Million Euro) is applicable to the breach under consideration. The amount depends on the breach of data protection law. If there are two or more breaches, and these attract different maximum amounts, the higher maximum amount will apply as this is the gravest breach.

The considerations applied in this section replicate GDPR Article 83 (2) and DPA 2018 sections 155 (3) (a), (c),(e), (f), (g), (h), (i) and (j), specifically:

- the nature, gravity, and duration of the failure;
- any action taken by the data controller or processor to mitigate the damage suffered by data subjects;
- any relevant previous failures by the data controller or processor;
- the degree of cooperation with the ICO, in order to remedy the failure and mitigate the possible adverse effects of the failure;
- the categories of personal data affected by the failure;
- the way the breach became known to the ICO, including whether, and if so to what extent, the data controller or processor notified the ICO of the failure;
- the extent to which the data controller or processor has complied with previous enforcement notices or penalty notices; and
- adherence to approved codes of conduct or approved certification mechanisms.

Step 2: Assessment of degree of culpability of the organisation concerned

In accordance with DPA 2018 section 155 (3) (d), the degree of culpability of the data controller or processor will be considered, taking into account technical and organisational measures implemented by them in accordance with DPA 2018 Sections 57, 66, 103 or 107. This will allow us to determine the degree of culpability that can be apportioned to the data controller or processor for the breach.

In accordance with DPA 2018 section 155 (3) (b) and GDPR Article 83 (b), we will also take into account the intentional or negligent character of the failure; specifically whether the organisation was intentional or negligent about its responsibility for the breach.

Step 3: Determination of turnover

DPA 2018 section 157 sets out the maximum amount of penalty that may be imposed with reference to turnover.

We will review the relevant accounts and obtain expert financial, or accountancy advice if required, to determine the amount of turnover (or equivalent for non-profit organisations such as the annual revenue budget and the financial means of individuals).

In circumstances where turnover or equivalent is minimal, we will give greater weight to factors considered in the other steps (such as dissuasiveness under step 8), particularly where there is a serious breach. Where there is a lack of cooperation in providing all relevant financial information, the panel will rely on the information available or otherwise give greater weight to factors considered in other steps (such as aggravating features under step 5).

Step 4: Calculation of an appropriate starting point

We will agree a starting point for the calculation of the penalty using the table below, based on the seriousness of the breach and the degree of culpability as determined at steps 1-2. We will then apply the appropriate percentage to the turnover or equivalent as determined at step 3.

Penalty starting point Standard Maximum Amount (SMA) (max of 2% or 10 Million Euro) Higher Maximum Amount (HMA) (max of 4% or 20 Million Euro)				
Seriousness: **Degree of culpability:**	**Low**	**Medium**	**High**	**Very High**
Low / No	**SMA** 0.125% **HMA** 0.25%	**SMA** 0.25% **HMA** 0.5%	**SMA** 0.375% **HMA** 0.75%	**SMA** 0.5% **HMA** 1%
Negligent	**SMA** 0.25% **HMA** 0.5%	**SMA** 0.5% **HMA** 1%	**SMA** 0.75% **HMA** 1.5%	**SMA** 1% **HMA** 2%
Intentional	**SMA** 0.375% **HMA** 0.75%	**SMA** 0.75% **HMA** 1.5%	**SMA** 1.125% **HMA** 2.25%	**SMA** 1.5% **HMA** 3%

Step 5: Consideration of relevant aggravating and mitigating features

In line with DPA 2018 section 155 (3) (k), and GDPR Article 83 (2) (k), we will consider any other aggravating and mitigating factors applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the breach.

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

Step 6: Consideration of financial means

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

This will be particularly important if an organisation's or individual's ability to pay is unclear or there has been a recent change in its financial, trading, or competitive status. We will ask the data controller or processor for information about its ability to pay, as appropriate.

Step 7: Assessment of economic impact

The ICO 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 it is needed, and that any action we take is proportionate. We must take this into consideration whenever we exercise a specified regulatory function.

The ICO will therefore, where appropriate, consider any economic impact on the wider sector, or related regulatory impact of the proposed penalty beyond the organisation or individuals we are serving the penalty on.

Step 8: Assessment of effectiveness, proportionality and dissuasiveness

The ICO will ensure that the amount of the fine proposed is effective; proportionate; and dissuasive and will adjust it accordingly, in line with DPA 2018 section 155 (3) (l) and GDPR Article 83 (1).

Step 9: Early payment reduction

The ICO will reduce the monetary penalty by 20%, if we receive full payment of the monetary penalty within 28 calendar days of sending the notice. However, this early payment discount is not available if a data controller or person decides to exercise their right of appeal to the First-tier Tribunal (Information Rights).

Does the penalty include cost recovery?

We do not consider our own investigative or regulatory costs in the penalty calculation.

Further reading

Penalty Notices DPA2018 (Sections 155 - 159)

DPA2018 Schedule 16

Deregulation Act 2015

Fixed penalties

Section 137 of the DPA 2018 states that data controllers are required to pay a registration fee to the ICO. There is more information on fees and how to pay them in the further reading section below.

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

(a) tier 1 (micro organisations) £400;

(b) tier 2 (small and medium organisations) £600; or

(c) 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 DPA2018 (Section 158)

Privileged communications

Section 133 of the DPA 2018 requires the ICO to publish guidance about how we will ensure that any privileged communications which are obtained by or which the ICO has access to are only used or disclosed so far as is necessary to carry out our functions. It also requires the ICO to publish guidance about how we will comply with restrictions or prohibitions relating to the obtaining or accessing privileged communications.

Sections 143(3)-143(4) and 147(2)-147(3) say that when requiring the provision or disclosure of information by an information notice or assessment

notice, that requirement will not apply to any privileged communications about data protection legislation. The ICO may obtain or have access to privileged communications in other circumstances. In those circumstances we will respect the confidentiality and sensitivities of the privileged communications and will handle them in accordance with the Attorney General's guidelines.

> **Further reading**
>
> Guidance about privileged communications DPA2018 (Section 133)
>
> Attorney General's guidelines on disclosure 2013

Effectiveness of regulatory action

Our Information rights 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 we've identified with individual organisations, sectors, or public authorities where we've identified and addressed systemic information rights problems.

> **Further reading**
>
> Information Rights Strategic Plan (IRSP)

Evaluation and next steps

We will keep this policy under review and evaluate it regularly and at least at the end of the Information rights strategic plan timeline. We will update it to reflect any amendments to legislation, including any implementation of an updated e-Privacy Regulation.