Regulatory Action Policy

ico.
Information Commissioner's Office

Information Commissioner's Office

Contents

Commissioner's foreword

As Information Commissioner, I'm responsible for regulating a wide range of legislation in the UK.

I'm both an educator and an ombudsman, and in most situations this is enough. But sometimes the carrot of education goes unheeded and regulators must use their stick – so I also have the ability to take enforcement action and apply sanctions when warranted.

My office has a range of enforcement and sanctioning powers, from light to severe – from letters warning against intended processing of data to monetary penalties of up to 4% of global turnover for the most serious and harmful contraventions.

These are significant powers, and we must use them predictably, consistently and judiciously. As Information Commissioner, I always try to select the most suitable regulatory tool by assessing the nature and seriousness of a failure, the sensitivity of the subject matter, whether and how individuals have been affected, the novelty and duration of the concerns, the public interest, and whether other regulatory authorities are already taking action on the matter. This all links back to my Information Rights Strategic Plan - my office's five-year programme of key regulatory priorities

Organisations should be able to predict how my office will carry out its regulatory activity, which is why we have developed this Regulatory Action Policy. We have drafted it with due regard to concerns raised during our public consultation in spring 2018. We'll continue to review the policy's effectiveness, and adjust it as needed. We'll also produce more communications for specific sectors to help them understand how the ICO will seek to regulate them.

I believe this regulatory action policy shows how the ICO acts both as a strong defender of individuals' information rights and as an enabler of organisations seeking to use data responsibly and safely. Those who are subject to ICO regulatory action should be in no doubt that we will pursue failures under the law in a way that is transparent, consistent and proportionate.

Ultimately my office exists to uphold individuals' information rights in the digital age. Our refreshed Regulatory Action Policy sets out how I will do this.

Elizabeth Denham
Information Commissioner

Overview

Our Regulatory Action Policy sits under the umbrella of our Information Rights Strategic Plan for 2017-2021[1] which sets out the Information Commissioner's mission to increase the trust the public has in government, public bodies and the private sector: trust in transparency, in the digital economy and in digital public service delivery.

The purpose of this Policy is to provide direction and focus for those we regulate, the public and our staff about our chosen approach to regulatory action. This will help ICO achieve the goals we set out in our Strategic Plan, and complements our International Strategy 2017-2021.

This Policy sets out a risk-based approach to taking regulatory action against organisations and individuals that have breached the provisions of the data protection, freedom of information and other legislation, set out in our Aims below. As with earlier versions of the policy it focusses on 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, on the one hand, data subjects are protected, while ensuring that, on the other hand, business is able to operate and innovate efficiently in the digital age. We will be as robust as we need to be 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.

[1] https://ico.org.uk/media/about-the-ico/documents/2014134/20170413icoinformationrightsstrategicplan2017to2021v10.pdf

Aims

This Policy seeks to:

- set out the nature of the ICO's various powers in one place and to be clear and consistent about when and how we use them[2];
- ensure that we take fair, proportionate and timely regulatory action with a view to guaranteeing that individuals' information rights are properly protected;
- guide the ICO and our staff in ensuring that any regulatory action is targeted, proportionate and effective; and
- assist delivery of the six goals of the Information Rights Strategic Plan and uphold information rights effectively for individuals in the digital age.

In addition, by issuing this Policy 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.[3]
- providing additional statutory guidance about how we propose to exercise our other enforcement functions.[4]
- fulfilling our statutory obligation[5] to provide guidance as to how we propose to:

  (a) 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

  (b) comply with restrictions and prohibitions on obtaining or having access to privileged communications which are imposed by an enactment.

[2] Although see also the ICO Prosecution Policy Statement in relation to 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.

[3] See S160(1) Data Protection Act 2018
[4] See S160(2) Data Protection Act 2018
[5] See S133 Data Protection Act 2018

- fulfilling our statutory obligation to produce and publish a document specifying the amount of the penalty for a failure to pay the data protection fees required under the Data Protection (Charges and Information) Regulations 2018.[6]

Objectives of regulatory action

When considering whether to take action, and in carrying it out, we will seek to meet the following five objectives:

Objective 1

To respond swiftly and effectively to breaches of legislation which fall within the ICO's remit, focussing on (i) those involving highly sensitive information, (ii) those adversely affecting large groups of individuals, and/or (iii) those impacting vulnerable individuals.

Objective 2

To be effective, proportionate, dissuasive and consistent in our application of sanctions, targeting our most significant powers (i) for organisations and individuals suspected of repeated or wilful misconduct or serious failures to take proper steps to protect personal data, and (ii) where formal regulatory action serves as an important deterrent to those who risk non-compliance with the law.

Objective 3

In line with legislative provisions, promote compliance with the law through the promotion of good practice and provision of targeted advice on how to comply with all aspects of the legislation.

Objective 4

To be proactive in identifying and mitigating new or emerging risks arising from technological and societal change.

Objective 5

To work with other regulators and interested parties constructively, at home and abroad, recognising the interconnected nature of the technological landscape in which we operate and the nature of data flows in the expanding digital economy. Our aim is to establish effective networks with other regulators to cut down on regulatory burden and red tape.

We will implement these objectives by exercising our statutory powers in the following ways:

[6] See S158 Data Protection Act 2018

- we will take action proportionately, we will exercise discretion as to when, in what manner, and to what extent enforcement is required;
- we will be selective when exercising this discretion, looking at the features and context of each case, as well as applying our resources more broadly to the areas of greatest risk and potential or actual harm to the community;
- we will apply our fining and other enforcement powers where they are effective, proportionate and dissuasive (to both the individual or organisation receiving the fine and more generally to those processing personal data;
- we will effectively deploy our intelligence products and technology to allow us to recognise and promptly tackle emerging threats; and
- we will seek to manage risks by sharing information effectively.

Where we are invoking our criminal prosecution powers we will do so by reference to the ICO Prosecution Policy Statement.

In applying the regulatory principles we will ensure that we always seek to meet our obligations under the Regulators' Code[7], the Victims' Code[8] and the Children Act 2004. We will also take account of the GDPR's requirements for greater consistency across Europe when determining the appropriate type and level of regulatory response in our data protection remit.

Legislative basis underpinning the ICO's regulatory activity

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

- Data Protection Act 2018 (DPA);
- General Data Protection Regulation[9] (GDPR);
- Privacy and Electronic Communications (EC Directive) Regulations 2003[10] (PECR);
- Freedom of Information Act 2000 (FOIA);

[7] Published in April 2014 and laid before Parliament in accordance with section 23 of the Legislative and Regulatory Reform Act 2006.
[8] The Code of Practice for Victims of Crime, also known as the Victims' Code, was established by the Domestic Violence, Crime and Victims Act 2004 and came into effect in 2006. It was revised in 2013 to reflect the commitments in the EU Victims' Directive 2012/29/EU, and updated again in 2015. The Victims' Code also reflects parts of the Human Trafficking and Child Sexual Exploitation EU Directives.
[9] Regulation (EU)2016/679
[10] S.I. 2003/2426

- Environmental Information Regulations 2004 (EIR)[11];
- Environmental Protection Public Sector Information Regulations 2009;[12]
- Investigatory Powers Act 2016;
- Re-use of Public Sector Information Regulations 2015[13];
- Enterprise Act 2002;
- The Network and Information Systems Regulations 2018 (NIS)[14]; and
- Electronic Identification, Authentication and Trust Services Regulation (e-IDAS)[15] [16].

Our regulatory activity

Our regulatory activity (and activity in support of regulatory activity) includes:

- conducting assessments of compliance with the DPA and GDPR (which we refer to in this Policy as the 'data protection legislation'), PECR, e-IDAS, NIS, FOIA and EIR;
- issuing information notices;
- issuing 'urgent' information notices under the DPA, requiring individuals, 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, if the recipient does not provide a full and timely response;
- issuing assessment notices under DPA;
- issuing 'urgent' assessment notices under the DPA, requiring controllers or processors to allow us to undertake an assessment of whether they are compliant with the data protection legislation, on not less than 7 days notice;
- issuing no-notice (or short notice) assessment notices under the DPA where we have reasonable grounds to suspect that the controller or processor has failed or is failing to comply with certain provisions of the

[11] S.I. 2004/3391
[12] S.I. 2009/3157. Also known as the INSPIRE Regulations 2009.
[13] S.I. 2015/1415
[14] S.I. 2018/506, implementing Directive (EU) 2016/1148
[15] Regulation (EU) 910/2014
[16] Readers should bear in mind that this list may be extended as new legislation is introduced following the publication of this Policy.

data protection legislation[17] or has committed or is committing an offence under the DPA, allowing us to undertake an assessment on less than 7 days notice;

- producing codes of practice about data sharing and direct marketing, and any other codes of practice that we are required to produce under the legislation we cover;
- conducting assessments of cross-border data transfers and corporate groups' binding corporate rules;
- overseeing data protection impact assessments;
- conducting audits and assessments under IPA and other information rights legislation;
- overseeing the establishment of data protection certification mechanisms;
- encouraging the development of codes of conduct, and accrediting bodies to monitor compliance with codes of conduct;
- requiring a controller or digital service provider to inform an individual of a personal data breach;
- issuing a warning where proposed action threatens non-compliance with data protection legislation;
- issuing a reprimand for infringements of relevant data protection legislation;
- issuing practice recommendations under FOIA and EIR and decision notices detailing the outcome of an ICO investigation into an individual's case under FOIA or EIR;
- issuing enforcement notices orders requiring specific actions by an individual or organisation to resolve breaches (including potential 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 legislation, on not less than 24 hours' notice;
- certifying contempt of court should an authority fail to comply with an information notice, decision notice or enforcement notice under FOIA and EIR;
- administering fines by way of penalty notices in the circumstances set out in section 155 of the DPA;

[17] Set out in S149(2) of the Data Protection Act 2018

- administering fixed penalties for failing to meet specific obligations (e.g. a failure to pay the relevant fee to the ICO); and
- prosecuting criminal offences before the courts.

We will 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 telephone contact centre, web chat and on our website.

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

Selecting the appropriate regulatory activity for breaches of information rights

We will adopt a selective approach to the action we take. When deciding whether and how to respond to breaches of information rights obligations, we will consider criteria including[18]:

- the nature and seriousness of the breach or potential breach (including, for example, whether any critical national infrastructure or service is involved);
- where relevant, the categories of personal data affected (including whether any special categories of personal data are involved) and the level of any privacy intrusion;
- the number of individuals affected, the extent of any exposure to physical, financial or psychological harm, and, where it is an issue, the degree of intrusion into their privacy;
- whether the issue raises new or repeated issues, or concerns that technological security measures are not protecting the personal data;
- the gravity and duration of a breach or potential breach;
- whether the organisation or individual involved is representative of a sector or group, raising the possibility of similar issues arising again across that group or sector if not addressed;
- the cost of measures to mitigate any risk, issue or harm;

[18] Note that this set of criteria is not intended to be exhaustive.

- the public interest in regulatory action being taken (for example, to provide an effective deterrent against future breaches or clarify or test an issue in dispute);
- whether another regulator, law enforcement bodies or competent authority is already taking (or has already taken) action in respect of the same matter; and
- in relevant cases, the expressed opinions of the European Data Protection Board.

We also reserve the right to take into account any aggravating or mitigating factors where relevant, for example[19]:

Aggravating Factors

- whether the attitude and conduct of the individual or organisation concerned suggests an intentional, wilful or negligent approach to compliance or unlawful business or operating model;
- whether relevant advice, warnings, consultation feedback, conditions or guidance from the ICO and/or the Data Protection Officer (for data protection cases) has not been followed;
- in data protection cases, whether the relevant individual or organisation is certified by a body that has been accredited under Article 43 of the GDPR or has failed to follow an approved or statutory code of conduct;
- the relevant individual or organisation's prior regulatory history, including pattern, number and type of complaints about the issue;
- the vulnerability, if any, of the individuals affected, in particular by virtue of their age or other protected characteristic under the Equality Act 2010;
- the state and nature of any protective or preventative measures and technology available, including by design;
- the manner in which the breach or issue became known to the ICO and, if relevant, failure or delay by the relevant individual or organisation to notify the ICO of the breach or issue; and
- any financial (including budgetary) benefits gained or financial losses avoided by the relevant individual or organisation, directly or indirectly.

Mitigating factors

- any action taken by a relevant individual or organisation to mitigate or minimise any damage (including delay) suffered by individuals;

[19] As above, it should be noted that this list of factors is not intended to be exhaustive.

- in data protection cases, whether the relevant individual or organisation has followed an approved or statutory code of conduct
- the state and nature of any protective or preventative measures and technology available; and
- early notification by the relevant individual or organisation to the ICO of the breach or issue.

As a matter of course, we will typically invite comments from those we regulate[20] about the application of regulatory action where are taking action at the upper end of the scale, save where it is inappropriate to do so (for example, where a matter is particularly urgent or there is a need for wider protection of others from harm).

In line with our commitment to transparency and accountability, we will be as open as possible about our regulatory, and, where relevant, enforcement work. We will normally publish details about the volume and types of cases we pursue and the outcomes we achieve. In particular, we will report on those relating to corrective measures, sanctions, fines or civil monetary penalties, enforcement notices or orders, fixed penalty notices and prosecutions. We may also publish case study examples to illustrate good practice or learning.

We will be particularly careful to ensure that redaction of confidential, personally sensitive or commercially sensitive information is properly considered when publishing details of specific cases. We will also set our internal service performance measures to focus on impacts and outcomes rather than any prescribed sanction or regulatory activity levels.

A hierarchy of regulatory action

We will consider each case on its merits and within the context of any compliance breach (or risk of such breach). However, as a general principle, the more serious, high-impact, intentional, wilful, neglectful or repeated breaches can expect stronger regulatory action. Breaches involving novel or invasive technology, or a high degree of intrusion into the privacy of individuals, without having done a full Data Protection Impact Assessment and taken appropriate mitigating action and/or which should have been reported to the ICO[21] but was not, can also expect to attract regulatory attention at the upper end of the scale.

[20] Such representations are invited from individuals and organisations against whom the ICO is considering taking enforcement action, rather than from complainants.
[21] See Art 36 GDPR

Our regulatory approach generally represents a range of measures. This spans observation, intelligence gathering and monitoring through to individual case and appeal considerations, as well as application of audit/assessment or inspection powers to better understand an issue, and, then, finally investigation and sanction where we need to look at and address the detail of an incident.

In this way, as issues or patterns of issues escalate in frequency or severity then we will use more significant powers in response. This does not mean however that we cannot use our most significant powers immediately in serious or high-risk cases where there is a direct need to protect the public from harm.

Our approach will also encourage and reward compliance. Those who self-report, who engage with us to resolve issues and who can demonstrate strong information rights accountability arrangements, can expect us to take these into account when deciding how to respond.

We will also provide opportunities for innovative products, services or concepts to be tested with appropriate regulatory oversight and safeguards, so that innovation and development is not over-burdened.

International regulatory action

Given the extent of international data flows and their importance to the economy[22], as well as the extra-territorial nature of the GDPR, we will take action in support of our International Strategy and in line with our cooperation and consistency mechanism obligations under the GDPR.

This approach means that in cases involving cross-border information flows we will liaise internationally with other supervisory authorities. We will do so to identify the most appropriate regulatory response, including identifying any lead authority or other concerned supervisory authorities under the GDPR (usually where the controller's 'main establishment' is based), as well as to share information to assist investigations, provide mutual aid and secure appropriate regulatory outcomes.

We already have a significant international standing, being an active participant in the:

- European Data Protection Board;
- British Islands and Irish Data Protection Authorities network;
- Common Thread Network;

[22] *The exchange and protection of personal data, A future partnership paper,* HMSO 2017

- Global Privacy Enforcement Network;
- International Conference of Data Protection and Privacy Commissioners;
- International Conference of Information Commissioners;
- Organisation for Economic Co-operation and Development;
- Unsolicited Communications Enforcement Network (formerly known as the London Action Plan); and
- Council of Europe Convention 108 signatories.

More details about these groups and their role is on our website.

In addition, we have direct contact with a range of data protection authorities on individual cases and systemic issues (such as the privacy issues arising from app development or connected toys). We share intelligence, information, threat analyses, tactics, guidance and learning with these groups. Where appropriate we coordinate our investigative and evidence gathering activity with these partners; this may be either jointly or individually depending on the circumstances of the case.

We also have operational protocols and memoranda of understanding with our international partners in support of this policy, and we will continue to keep these updated. We publish more information about them on our website [link].

Working with others to take effective action

In addition to our international work we often work with a range of other regulators and agencies to deliver our remit. This includes:

- National Cyber Security Centre, in our role as a NIS competent authority, and in the immediate response phase to cyber-attacks which lead to breaches of personal data;
- other NIS competent authorities, such as the Drinking Water Authority, Office of Communications, and Civil Aviation Authority;
- law enforcement, including the National Crime Agency, in cases involving the theft or criminal misuse of personal data; and
- sector and consumer regulators, including, the Financial Conduct Authority and the Competition and Markets Authority Competitions and Marketing;

As with our international work we share intelligence, threat analyses, insight, and tactics with these groups, and we refer relevant cases where they fall within their jurisdiction as well as our own. Where we undertake joint regulatory

or investigative work we coordinate our activity to ensure a proportionate burden on those being regulated (e.g. minimising duplication of evidence gathering/information requests). These arrangements are set out in protocols and memoranda of understanding published on our website.

We also do additional work in support of our regulatory action where it is necessary to give effect to that action. For example, where a company seeks to avoid a financial penalty through complex liability structures or by dissolution, we will pursue matters via winding-up orders or by referral to the Insolvency Service. We have achieved success in obtaining disqualification of directors and winding-up orders to disrupt those who repeatedly break the rules, and we will expand our work in this area.

Statutory Guidance:

This section applies in addition to the general guidance and policies set out in this document as to our approach to regulatory action.

When we will issue Information Notices

An information notice is a formal request for a controller, processor or individual to provide us with information, within a specified time frame, to assist us with our investigations. In some circumstances it may be a criminal offence to provide a response which is false in any material respect.

We may serve an information notice at our discretion in any investigation. We will have regard to what action is appropriate and proportionate, and criteria 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 utility of requiring a formal response within a defined time period;
- the utility 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, in particular whether or not to issue an ‘urgent’ information notice, we will have regard to what action is appropriate and proportionate and criteria including:

- the extent to which urgent investigation may prevent or limit the risk of serious harm to individuals or serious intrusion into their privacy. For example requesting an early report on a serious data security breach in

order for the ICO to advise the controller on and validate appropriate notification to data subjects and appropriate mitigation of the breach.
- 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 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 the ICO obtain information under an urgent information notice (which may be by court order), prior to an appeal being heard by the Information Tribunal;
- 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.

If a recipient of an information notice does not fully respond within the applicable time period, whether urgent or not, the Commissioner will promptly apply for a court order requiring a response. The Commissioner may decide not to make such application, having regard to 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, the ICO may decide it has sufficient evidence to move to an enforcement action in any event; and
- the public interest.

The Commissioner will also consider whether or not to issue a Penalty Notice (see below).

When we will issue Assessment Notices

The DPA contains a provision for the ICO to issue an 'assessment notice'[23]. This is, essentially, a notice which is issued by the ICO to a controller or processor to allow us to investigate whether the controller or processor is compliant with data protection legislation. The notice may, for example, require the controller

[23] Section 146 of the DPA

or processor to give us access to premises and specified documentation and equipment.

We may serve an assessment notice at our discretion in any investigation into compliance with the data protection legislation. We will have regard to what action is appropriate and proportionate, and criteria including:

- where we have conducted a risk assessment or other regulatory action, there is a probability that personal data is not being processed in compliance with the data protection legislation, together with a likelihood of damage or distress to individuals;
- it is necessary to verify compliance with an enforcement notice;
- communications with or information (e.g. news reports, statutory reporting or publications) about the controller or processor suggest that they are not processing personal data in compliance with the data protection legislation; and
- the controller or processor has failed to respond to an information notice within an appropriate time.

When determining the risks of non-compliance we will consider one or more of the factors for regulatory action. We will also consider other relevant information, such as reports by whistle-blowers, and any data privacy impact assessments that may have been carried out.

When deciding the period for compliance with assessment notices, in particular whether or not to issue an ‘urgent’, ‘no-notice’ or ‘short-notice’ assessment notice, we will have regard to what action is appropriate and proportionate, and criteria 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 the ICO gain access to its premises and data processing activities urgently, without notice or on short notice, and without the opportunity to appeal and/or for an appeal to be heard by the Information Tribunal;

- 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.

Assessments of documents, including 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 obligations have been met under the legislation, and the governance controls in place to measure compliance.

Although not an exhaustive list this could include, for example:

- Strategies
- Policies
- Procedures
- Guidance
- Codes of practice
- Training material
- Protocols
- Frameworks
- Memoranda of understanding
- Contracts
- Privacy statements
- Privacy impact assessments
- Control data
- Job descriptions

We may also need access to specified personal data or classes of personal data, and to evidence that it is being handled in compliance with the policies and procedures which ensure compliance with the legislation. The level of access will only be enough to assess compliance.

We do require access to information which:

- is subject to legal professional privilege (see below);
- has a high level of commercial sensitivity;
- is exempt information as defined by section 23 FOIA (information supplied by, or relating to bodies dealing with security matters); or

- is exempt from the DPA, by virtue of a national security certificate[24].

We recognise that there might also be legitimate concerns about other information which relates to issues of national security, international relations or sensitive activities. In these cases it will generally be possible to audit data protection compliance without access to such information. Where it is necessary and appropriate, we will ensure that properly vetted members of staff inspect such information. We have memoranda of understanding with relevant agencies to provide access and understanding of this type of material.

Individuals can contact us to request that, if an assessment notice requires access to such information, this access be limited to the minimum required to adequately assess their compliance with the legislation. They may also request other access conditions. Such requests must be made 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.

Inspection and examinations during assessments

Inspections and examinations are key review elements of the assessment. They help us to identify objective evidence of compliance, and how policies and procedures have been implemented.

These reviews of personal data, and associated logs and audit trails, may consider both manually and electronically stored data, including data stored centrally, locally and on mobile devices and media.

We use these reviews to evaluate how an organisation:

- obtains, stores, organises, adapts or alters information (eg policies and procedures) 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

[24] Section 27 of the DPA

- weeds and destroys personal data.

The review may also cover management/control information, to monitor and record how personal data is being processed, and to measure how a controller meets their wider obligations under the legislation.

The review may evaluate physical and IT-related security measures, including how personal data is stored and disposed of.

The 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 by auditors. If information is held electronically we may require the controller to provide manual copies or facilitate direct access.

Any direct access would be limited to the identified records, would only be done locally and would be for a limited and agreed time.

Data reviewed as part of the review and evaluation process, but not specifically identified in the assessment notice, may only be taken off the controller's site with the controller's permission.

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 and/or awareness of regulatory obligations. Departmental managers, operational staff, support staff (e.g. IT staff, security staff) as well as staff involved with information and information governance may be interviewed.

Where possible we will schedule and agree interviews with the controller or processor before the on-site audit. We will give a schedule of areas to be covered before the audit, and will discuss and agree the level and grade of staff to be interviewed (e.g. managers, operational staff etc.). Individuals should be advised by the target organisation in advance of their required participation.

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 a number of staff in an interview – where, for example, there are shared responsibilities. Auditors will take notes during 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 recommended.

We will make every effort to restrict interviews to staff identified within the agreed schedule. But when it becomes clear during an audit that access to additional staff may be necessary, we will arrange this with the consent of the 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 in assessing 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, the interview will be halted.

Individuals' names may be used in distribution lists and the acknowledgements sections of reports, but they will not be referenced in the body of any report. Job titles may be used where appropriate.

Publication of assessment reports

We will follow the procedure set out in our Communicating our Regulatory and Enforcement Activity Policy when publishing assessment reports.

If a recipient of an information notice does not fully respond within the applicable time period, whether urgent or not, the Commissioner will promptly apply for a court order requiring a response. The Commissioner may decide not to make such application, having regard to 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, the ICO may decide it has sufficient evidence to move to an enforcement action in any event; and
- the public interest.

If a controller or processor fails to comply with an Assessment Notice, the Commissioner will consider whether or not to issue a Penalty Notice (see below).

Privileged communications

We do not require access to information which is subject to legal professional privilege. Where we receive such privileged information we will respect the confidentiality of this information and any particular sensitivities. We will handle all such privileged communications in accordance with the Attorney Generals Guidelines.

When we will issue Enforcement Notices

Enforcement notices may be issued in the circumstances set out in section 149 of the DPA or Regulation 17 of the NIS Regulations. For example, where a controller or processor has breached one of the data protection principles, where a certification provider or monitoring body for a code of conduct is failing to meet their obligations, or where a relevant digital service provider has suffered a failing as set out in Regulation 17 of the NIS Regulations.

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 and/or remedy a breach. Failure to comply with an enforcement notice invites further action, including the possibility of the ICO issuing a civil monetary penalty.

Enforcement notices will usually be appropriate where specific correcting action (or its prevention) may be required. Although this is not an exhaustive list, an enforcement notice may be required in such circumstances as:

- repeated failure to meet information rights obligations or timescales for them (e.g. repeatedly delayed subject access requests);
- where processing or transfer of information to a third country fails (or risks failing) to meet the requirements of the data protection legislation;
- where there is an ongoing NIS incident requiring action by a digital service provider;

- there is a need for the ICO to require communication of a data security breach to those who have been affected by it; or
- there is 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;
- how to report that the action has been 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 have regard to the factors set out above, including the presence of any mitigating or aggravating factors.

Timescales set out in an enforcement notice will usually reflect the imminence of proposed action that could lead to a breach of obligations, the severity and scale of any breach/failings, and the feasibility (including lead times) of any correcting measures or technology.

In addition, when deciding whether or not to issue an 'urgent' enforcement notice, and in deciding the period for compliance with such notice, we will consider whether urgent action by the recipient (to take specific steps or to stop specific processing of personal data) is appropriate and proportionate having regard to criteria including:

- 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 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.

If a controller or processor fails to comply with an enforcement notice, the Commissioner will also consider whether or not to issue a Penalty Notice (see below).

Penalty Notices

The ICO's 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 information rights or legislation, as well as act as an effective deterrent.

Our decision whether to impose a penalty at all; **and** the decision as to the amount of the penalty in a case will involve consideration of the following factors:

- the nature, gravity and duration of the failure;
- The intentional character of the failure or the extent of negligence involved;
- any action taken by the controller or processor to mitigate the damage or distress suffered by the data subjects;
- the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by the controller or processor in accordance with the GDPR and sections 57, 66, 103 and 107 of the DPA;
- any relevant previous failures by the controller or processor;
- the degree of co-operation with the Commissioner, in order to remedy the failure and mitigate the possible adverse risks of the failure;
- the categories of personal data affected by the failure;
- the manner in which the infringement became known to the Commissioner, including whether, and if so to what extent, the controller or processor notified the Commissioner of the failure;
- the extent to which the controller or processor has complied with previous enforcement notices or penalty notices;
- adherence to approved codes of conduct or certification mechanisms;
- any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly);
- whether the penalty would be effective, proportionate and dissuasive.

When a Penalty Notice will be appropriate

In the majority of cases we will reserve our powers for the most serious cases, representing the most severe breaches of information rights obligations. These will typically involve wilful, deliberate or negligent acts, or repeated breaches of information rights obligations, causing harm or damage to individuals. In considering the degree of harm or damage we may consider that, where there

is a lower level of impact across a large number of individuals, the totality of that damage or harm may be substantial, and may require a sanction.

This means that each case will be assessed objectively on its own merits. But our hierarchy and risk-based approach mean that it is more likely that a penalty will be imposed where, for example:

- a number of individuals have been affected;
- there has been a degree of damage or harm (which may include distress and/or embarrassment);
- sensitive personal 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.;
- wilful action (including inaction) is a feature of the case;
- there has been a failure to apply reasonable measures (including relating to privacy by design) to mitigate any breach (or the possibility of it); and
- there has been a failure to implement the accountability provisions of the GDPR.

When oral representations will be appropriate

Before issuing a penalty we will advise the target that we intend to levy a penalty by issuing a notice of intent (NOI). The NOI will set out the circumstances of any breach, our investigation findings and the proposed level of penalty, along with a rationale for the penalty and any proposed enforcement notice requirements.

Representations will be taken from the proposed target about the imposition of the penalty and its level. The target will be allowed at least 21 calendar days to make these representations.

In addition, we may allow an organisation or individual subject to an NOI to submit representations orally during a face-face meeting at our office. 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;
- the integrity of any technical witness evidence is in dispute;

- there is a requirement to make reasonable adjustments under the Equality Act 2010; or
- the consideration of 'harm' elements of a case would benefit from evidence from those affected.

During these meetings, representatives of the target of the NOI are able to explain in person how the privacy concerns and breaches occurred, submit mitigating factors, what they have (or plan to do) to achieve compliance and the reasons why they believe that the ICO should not take the intended regulatory action. A request for a reduction in the size of the penalty may also be submitted during the oral representations.

If an organisation or individual thinks that their circumstances warrant oral representations of this nature, they can explain why they think this extra step is justified in their written representations. In particular, the ICO will need to understand what oral representations will add to the regulatory process. We will then decide whether or not to invite the target 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.

Where appropriate, we will also have regard to representations (including from any Concerned Supervisory Authorities elsewhere in the EU where the ICO is the lead Supervisory Authority or the Data Protection Board itself) under the cooperation and consistency mechanisms of the GDPR in setting the final amount of any penalty. These representations will be taken after the consideration of representations of the target of the penalty but before the final setting of any penalty level and following the procedures set out in relevant Data Protection Board rules of procedure.

For very significant penalties (expected to be those over the threshold of £1M) a panel comprising non-executive advisors to the Commissioner's Office may be convened by the Commissioner to consider the investigation findings and any representations made, before making a recommendation to the Commissioner as to any penalty level to be applied. It will be the Commissioner's final decision as to 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. We will also advise those subject to penalties of any relevant rights of appeal that apply to their case.

What will be the amount of any penalty

Where we have discretion to set the amount of any penalty in the context of our regulatory work, we will approach setting any penalty level, within the legislative bands, on the basis of the following mechanism:

Step 1. An 'initial element' removing any financial gain from the breach.

Step 2. Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 155(2)-(4) of the DPA.

Step 3. Adding in an element to reflect any aggravating factors.

Step 4. Adding in an amount for deterrent effect to others.

Step 5. Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship).

In data protection cases (including NIS cases) involving failures to meet data security obligations we will consider the breach separately from the failure to report. In all other cases we will adopt a 'whole case' approach when setting the penalty level.

Generally, the amount will be higher where:

- vulnerable individuals or critical national infrastructure are affected;
- there has been deliberate action for financial or personal gain;
- advice, guidance, recommendations or warnings (including those from a data protection officer or the ICO) have been ignored or not acted upon;
- there has been a high degree of intrusion into the privacy of a data subject;
- there has been a failure to cooperate with an ICO investigation or enforcement notice; and
- there is a pattern of poor regulatory history by the target of the investigation.

Fixed penalties

Certain legislation provides for set penalties to be applied 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 those penalties in accordance with the law.

For the purposes of section 155 of the DPA, the fixed penalty payable by a controller for any type of failure to pay a data protection fee in accordance with the Data Protection (Charges and Information) Regulations 2018, are [25]:

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

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

(c) tier 3 (large organisations), is £4,000.

We reserve the right to increase this amount up to a statutory maximum of £4,350[26] for data controllers in respect of a failure to provide the ICO with sufficient information to determine the appropriate fee/exemption, depending on aggravating factors (for example, a failure to engage or co-operate with the ICO).

Cost recovery

We will not consider our own investigative or regulatory costs in the application of a penalty calculation. All monetary penalties will be payable for the benefit of HM Treasury and the Consolidated Fund.

NIS provides that the ICO should develop, by 2020, a mechanism to recover its costs in regulating Digital Service Providers (DSPs). The ICO will produce separate guidance on how it proposes to do this, in consultation with relevant DSPs.

Effectiveness of regulatory action

Our Information Rights Strategy sets out the measures we apply to the effectiveness of our work.

We will 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 identified with individual organisations,

[25] The tiers are as defined in the Data Protection (Charges and Information) Regulations 2018

sectors or public authorities where systemic information rights problems have been identified and addressed.

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, and once the final settlement between the EU and the UK post-Brexit is confirmed.