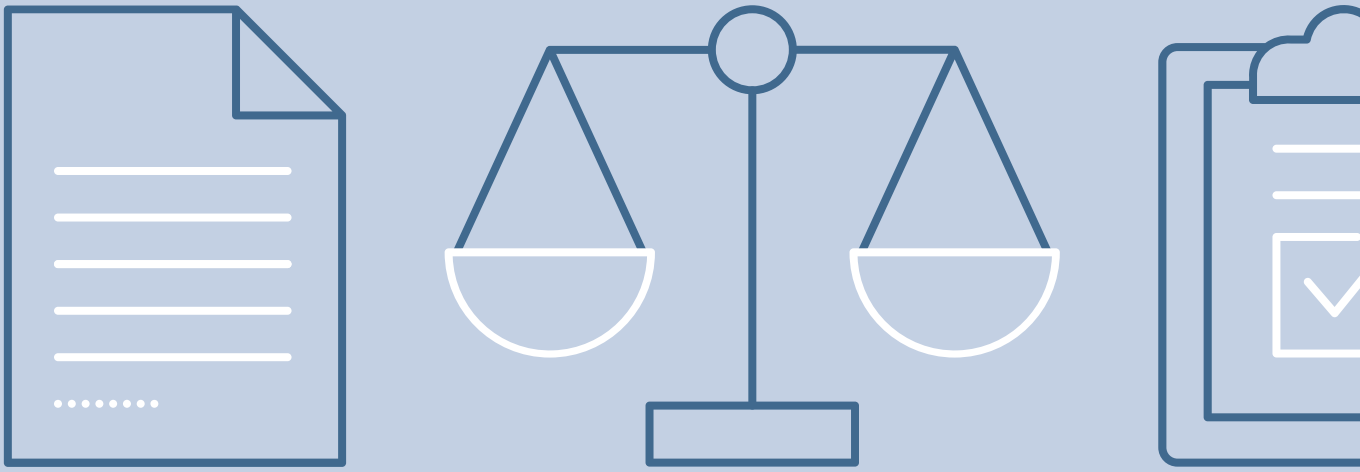
Draft

Regulatory action policy



ico.
Information Commissioner's Office

Contents

Foreword

We will insert a foreword here in the final version of the regulatory action policy.

Part A: The ICO in context – explaining our role and approach to regulatory action

About this policy

What is the purpose of this policy?

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

The statutory guidance on our regulatory action (statutory guidance) focuses on our data protection obligations and provides information about how the ICO exercises its powers under the Data Protection Act 2018 (DPA 2018).

This wider policy sets out our general approach when using our regulatory powers under the range of legislation we monitor and enforce. This includes the regimes that do not carry a legal obligation for formal guidance. It is split into two parts; Part A and Part B.

Part A focuses on our role and explains how we:

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

Part B focuses on the individual pieces of legislation we are responsible for and the specific regulatory action we can take for each piece of legislation. The structure of these sections is the same and you can read them in isolation if you prefer.

By regulatory action, we mean any action we take in exercising our wider discretionary powers under the legislation that we have a responsibility to monitor and enforce. This includes giving advice, writing guidance, auditing, assessing, enforcing against systemic breaches of the rules, warning and prosecuting. This policy sets out below our responsibilities and how we use our actions to encourage organisations to comply with the laws we monitor.

The purpose of this document is to provide clarity to those we regulate and the public about our approach to selecting and taking regulatory action. This helps us to achieve the goals we set out in our Strategic Plan.

Like all regulators and law enforcement agencies, the ICO's resources are not limitless. We receive an allocation of grant-in-aid from the UK government for some specific tasks, such as considering freedom of information appeals. However, the majority of our funding comes from the data protection fee, paid by hundreds of thousands of small businesses in the UK. This document sets out our risk-based approach to taking regulatory action. This involves working with

organisations and members of the public that may fail to meet the provisions of the laws we regulate or who may need support or guidance to comply. In doing this, our focus is usually on areas of high risk, or circumstances where non-compliance could do the most harm.

Our approach aims to help create an environment that protects data subjects and supports access to information, while ensuring that businesses, charities and public services are able to operate and innovate efficiently in the digital age. We want to support organisations to use, hold and share information in ways that are as transparent and accountable as possible. We recognise and support the role transparency and accountability play in increasing public trust.

We are as robust as we need to be in upholding the law, whilst ensuring that commercial businesses and public services are not worried that we may use our sanctions disproportionately. We work with others, for example other regulators, where it makes sense to do so, including where it is necessary to achieve better outcomes or protections for data subjects.

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

- explain our regulatory responsibilities;
- show how we exercise our regulatory responsibilities effectively, consistently and proportionately, being fair and clear about which types of action we use, and when and how we use them;
- explain how we take timely regulatory action with a view to properly protecting the public's information rights while supporting innovation and enterprise; and
- provide clarity to those we regulate and the wider public about our approach to regulatory action.

Who is this policy for?

This policy is to inform both people and organisations who collect, use, store and share information about our responsibiltiies to promote compliance and our powers to enforce UK information rights legislation.

Which legislation does this policy cover?

We can take various regulatory actions under the following legislation:

- Data Protection Act 2018 (DPA 2018);
- UK General Data Protection Regulation (UK GDPR);
- Freedom of Information Act 2000 (FOIA);
- Re-use of Public Sector Information Regulations 2015;
- Environmental Information Regulations 2004 (EIR);

- Environmental Protection Public Sector Information Regulations 2009 (INSPIRE Regulations);
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR);
- The Network and Information Systems Regulations 2018 (NIS);
- Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (eIDAS);
- Enterprise Act 2002; and
- Investigatory Powers Act 2016.

Further reading

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

ICO Prosecution Policy Statement

Data Protection Act 2018

Guide to the UK GDPR

Freedom of Information Act 2000

Re-use of Public Sector Information Regulations 2015

Environmental Information Regulations 2004

Environmental Protection Public Sector Information Regulations 2009 (The INSPIRE Regulations)

Privacy and Electronic Communications (EC Directive) Regulations 2003

Network and Information Systems Regulations 2018

Electronic Identification and Trust Services for Electronic Transactions Regulations 2016

Enterprise Act 2002

Investigatory Powers Act 2016

How we help you comply with the legislation we monitor and enforce

We want people and organisations to get things right when using, handling, sharing and storing information, including personal data. We only use enforcement action when necessary. We provide a number of services to help people comply with the law and answer questions about the legislation we regulate, for example:

- We provide a suite of guidance products to help organisations and the public know how to comply with or exercise their rights under the law and we update our guidance as things change. Our suite of guidance covers topics including how to correctly handle information requests, the public's data rights, how artificial intelligence should interact with personal data and how you should process the most sensitive data.
- We provide advice explaining how organisations can better comply with the law.
- We attend and host events and conferences to raise awareness of our work and the legislation we regulate and our skills and experience are in high demand from external stakeholders.
- We run a contact centre where people can get in touch online or over the phone with specific questions and seek tailored advice.
- We produce Opinions to raise awareness and promote information rights.
- We produce blogs, newsletters, webinars and use social media to raise awareness and promote information rights.
- We publish Decision Notices about Access to Information appeals we have received so public bodies can better understand how to handle the requests they receive.
- We also use our Decision Notices, and where needed Practice Directions, to identify systemic performance issues and remedial actions for public authorities.
- We run a hub for small businesses where they can access information tailored to their needs. In 2019 we created a specific department dedicated to supporting small to medium businesses, which produces specific guidance products for the SME community.
- We support organisations to implement new ideas safely by reviewing their data protection impact assessments (DPIAs). We've supported a range of sectors to complete DPIAs including utility companies, transport providers, local authorities, charities and technology and communications companies, as well as advising on DPIAs relating to COVID-19.
- We run a grants programme funding innovative projects which look at new areas of data protection. So far, we have funded innovative research and

tool development in areas such as children's privacy, genomic data, biometric technologies and smart home devices.

- Our relationship management service helps us to support larger organisations who we have regular contact with. This enables us to get key messages out quickly and effectively and coordinate our work with key stakeholders.
- We also help organisations to test new and innovative data protection concepts in a safe environment through our sandbox. We've completed a diverse range of projects, which include supporting the higher education sector in developing new tools, based on data, to intervene and support student mental health. We are also supporting the NHS in their response to COVID-19 and their development of a central mechanism to allow people to get involved with researchers undertaking vaccine trials.
- We collaborate with other regulators on initiatives that bring about innovation. Our permanent Innovation Hub provides expert support to businesses participating in these initiatives, helping them build data protection compliance into their projects at an early stage. Our Innovation Hub also collaborates with regulatory bodies to help them embed information rights practie in their own procedures when supporting business innovation.
- We investigate key issues of concern to the public and produce reports which set out our findings, share learning and make recommendations about improving practice in the future. These reports set important precedents and provide advice for organisations about how they can use data appropriately. For example, we investigated and reported on the way the police use the data they extract from victims' mobile phones to investigate alleged crimes. We have also reported on the case for extending Freedom of Information to private companies providing public services and investigated the way credit reference agencies use personal data for marketing.

You can find out more about the work listed above in our annual report which provides key information about our activities each year.

Further reading

What we do for organisations

ICO guide to the Sandbox

ICO innovation hub

ICO suite of guidance

Action we've taken

Annual reports | ICO

Our legal responsibilities

What legal responsibilities do we have outside our regulatory responsibilities and how do we meet them?

As a public authority, we have a number of obligations and commitments that guide our regulatory activities and our work with other regulators. Meeting these commitments ensures we are a responsible regulator that treats people fairly and with respect.

- **The Regulators' Code**

  We must follow the Regulators' Code as our responsibilities are specified by order under section 24(2) of the Legislative and Regulatory Reform Act 2006. In adhering to this code, we aim to:

  - support and engage with those we regulate;
  - share information;
  - provide clear guidance; and
  - act transparently and in an accountable manner.

- **Code of Practice for Victims of Crime**

  In the context of our criminal enforcement responsibilities, we adhere to the Code of Practice for Victims of Crime and treat victims of crime in a respectful, sensitive, tailored and professional manner without any kind of discrimination.

- **The Deregulation Act 2015**

  We must consider the desirability of promoting economic growth when exercising our regulatory responsibilities in accordance with our duties under the Deregulation Act (with the exception of our regulatory functions under the Freedom of Information Act 2000). We must ensure that we only take regulatory action when we need to and that any action we do take is proportionate.

- **The Small Business, Enterprise and Employment Act 2015 and the Enterprise Act 2016**

  The business impact target (BIT) assesses the economic impact of regulation on businesses and aims to reduce the regulatory burden. The Small Business, Enterprise and Employment Act 2015 and the Enterprise Act 2016 requires regulators, including the ICO, to assess and report the economic impact of our regulatory activity on businesses.

- **The Equality Act 2010**

  We commit to promoting equality and diversity in all we do and aim to eliminate barriers that prevent people accessing our services or

employment opportunities with us. Under section 149 of the Equality Act (public sector equality duty), we must consider the need to eliminate discrimination and advance equality of those with relevant protected characteristics. These are age, disability, race, gender reassignment, pregnancy and maternity, religion, sex and sexual orientation.

Furthermore, under section 75 Northern Ireland Act 1998, in carrying out our responsibilities to Northern Ireland, we must promote equality of opportunity for people of different political opinion and for people with dependants.

- **Children's rights**

  We are fully committed to the principles in the United Nations Convention on the Rights of the Child, in particular acting in the best interests of children. These are underpinned in UK legislation and policies including the Children Act 1989 and the Children Act 2004.

  We are also committed to providing guidance to those we regulate about privacy standards that they should adopt when processing children's personal data. We produced a statutory code of practice on age-appropriate design for providers of information society services (ISS) that process personal data and are likely to be accessed by children. We often refer to this as the Children's Code.

- **Public law principles**

  We are committed to exercising our responsibilities in accordance with public law principles by acting lawfully, rationally, proportionately and fairly.

Further reading

Regulators' Code

Code of Practice for Victims of Crime in England and Wales

Deregulation Act 2015

Small Business, Enterprise and Employment Act 2015

Enterprise Act 2016

Equality Act 2010

Children Act 2004

Children's Code hub

Human Rights Act 1998

How do we meet our obligations to support economic growth?

The ICO has a statutory duty under the Deregulation Act 2015 to take into account the desirability of promoting economic growth. Furthermore, we have an obligation under the Regulators' Code to support economic growth.

We meet these obligations by ensuring that we only take action when we need to, and any action is proportionate, lawful, fair and rational. We achieve this in a range of ways, as explained below.

When exercising our regulatory responsibilities, we consider how we can support or enable innovation and growth for compliant organisations. We seek to understand and minimise negative economic impacts and compliance costs, promote greater regulatory certainty and encourage and promote compliance.

We are committed to developing the knowledge and understanding of our staff in relation to those we regulate, and enabling them to choose proportionate and effective approaches to regulation. One notable way we do this is via our regulatory policy methodology guidance which emphasises the importance of understanding the impacts of our actions and conducting proportionate impact assessments. We seek to maximise our impact, for example by taking action where we consider the risks and harms to be the greatest.

As noted above, we offer clear, practical guidance and advice to organisations, explaining and helping them to meet their legal obligations, which serves to support innovation and economic growth. This includes specific advice for small organisations through our SME Service Hub, as well as our SME helpline and live chat services, easy-to-follow advice, toolkits, checklists, podcasts and FAQs. Our regulatory sandbox and innovation hub support organisations' innovation in the use of data, while our grants programme encourages innovation in privacy more generally.

We aim to provide appropriate, fair and straightforward ways for the public, organisations and others to engage in our processes, including the development of regulatory policy. We work with organisations to consider the impacts on their businesses and the wider economy, explaining our proposals and decisions and providing appropriate opportunities for consultation and dialogue.

What other ICO policies and strategies do we have?

This policy sits alongside our other policies and strategies, which set out how we perform our duties within the legislation we are responsible for.

How do we make regulatory policy?

It is the role of government to set the legislative and policy framework for data protection and information rights. It is our role to independently apply regulation within this framework.

Regulatory policy is about how, within these parameters, we identify issues, decide whether or not we should take action and, if so, what our options are. Our regulatory policy methodology sets out a systematic, evidence-based approach to support decision-makers.

This can include deciding how to balance trade-offs between competing priorities, how to interpret legal provisions and identifying the challenges and opportunities of emerging technologies and business models.

It is important that we, as the regulator, are independent as government are also subject to information rights regulation. Article 52 of the UK GDPR specifically states that we must be able to do our work fairly and without political interference.

We cannot legislate, but we can make recommendations to government (including the UK government and devolved administrations) if we think there is a good case for legislative change in any of the areas we regulate. In such cases, the government's ability or willingness to make such changes, and the timescales involved, determine some of the constraints on our policy making.

We work in a constantly evolving environment with increasingly complex approaches to data processing and complicated associated ecosystems. It can be challenging to identify the implications of these developments within the regulatory framework. We are therefore working to identify the skills that our policy professionals need to deal with the increasing complexity of data protection and information rights. We're also developing a range of interventions to ensure that we have the right professional development opportunities and career paths in place.

Further reading

Our strategies and plans

ICO policies and procedures

ICO Regulatory Policy Methodology

Our approach to our regulatory responsibilities

How do we prioritise our work?

Prioritising our work enables us to make the best use of our resources. To do this we have a prioritisation framework. The prioritisation framework typically takes account of a number of factors including:

- the likely impact of our actions, including consideration of risks, harm and opportunities; and
- alignment with our strategic priorities, including consideration of whether the ICO is best placed to act or should work in collaboration with others.

We balance these considerations against the risks. This includes the likelihood of success, legal, financial and reputational risks, and the resources that the work might involve. We also take account of the proportionality of resource implications in light of the intended outcomes.

We consider these issues in the round and on a case-by-case basis, taking account of the available evidence, exercising judgement where necessary and including other relevant factors where appropriate, including the public interest. Depending on the circumstances, we may use one or more risk assessment tools, and weigh evidence from a wide range of sources, including:

- complaints we receive;
- audit findings;
- outcomes of previous investigations;
- policy work;
- breach reports;
- intelligence;
- our work with other regulators; and
- consumer research such as our annual track survey of UK residents and wider national and international engagement with the public and stakeholders.

How do we approach our regulatory responsibilities?

We aim to respond swiftly and effectively to serious breaches of legislation which fall within our remit.

In some cases, we do this by engaging with a sector or issue, or through education and information sharing with the public to help them protect themselves or exercise their rights. This includes giving advice, issuing guidance or by publishing a formal Opinion, warning or reprimand. When we take enforcement action, we aim to be effective, proportionate, dissuasive, fair and consistent, in line with our obligations under the Regulators' Code. Our statutory

guidance sets out the situations in which we are likely to exercise our compulsory powers under the data protection legislation.

In respect of our obligations more generally, when deciding whether and how to respond to information rights breaches, we consider each case individually and take into account a number of factors including:

Aggravating factors

- the attitude and conduct of the person or organisation concerned suggests an intentional, wilful or negligent approach to compliance or an unlawful business or operating model;
- the breach or potential breach is particularly serious (for example, whether it involves any critical national infrastructure or service. Critical national infrastructure includes buildings, networks and other necessary systems that provide essential public services, for example energy, finance, telecoms and water services);
- a high degree of damage to the public (which may include distress or embarrassment);
- the data protection legislation breaches resulted in a relatively low degree of harm, but it affected many people;
- the person or organisation significantly or repeatedly failed to follow the good practice set out in the codes of practice we are required to promote;
- the person or organisation did not follow relevant advice, warnings, consultation feedback, conditions or guidance from us or the data protection officer (for data protection cases);
- the person or organisation failed to comply with an information notice, an assessment notice or an enforcement notice;
- the breach concerns novel or invasive technology;
- in data protection cases, if the person or organisation is certified by an accredited body under Article 43 of the UK GDPR, and failed to follow an approved or statutory code of conduct;
- the person or organisation's prior regulatory history, including the pattern, number and type of complaints about the issue and whether the issue raises new or repeated concerns that technological security measures are not protecting the personal data;
- the vulnerability, if any, of the affected people, due to their age, disability or other protected characteristic under the Equality Act 2010 (or section 75 Northern Ireland Act 1998);
- the breach involves special category data or a high level of privacy intrusion;
- the state and nature of any protective or preventative measures and technology available, including by design;

- the way we found out about the breach or issue and, if relevant, failure or delay by the person or organisation to notify us of the breach or issue; and
- if the person or organisation, directly or indirectly, gained any financial (including budgetary) benefits or avoided any financial losses.

Mitigating factors

- if the person or organisation notified us of the breach or issue early and has been open with us;
- any action the person or organisation took to mitigate or minimise any damage (including delay) that people suffered;
- any early action the organisation took to ensure future compliance with a relevant code of practice;
- in data protection cases, whether the person or organisation followed an approved or statutory code of conduct;
- the state and nature of any protective or preventative measures and technology available; and
- whether the person or organisation co-operated fully with us during any investigation.

Other factors we may consider

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

We generally invite comment from those we regulate about the application of regulatory action which directly affects them, except if it is inappropriate to do so. For example, if 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 are, where appropriate, open about our regulatory and enforcement work. We normally

publish details about the volume and types of cases we pursue and the outcomes we achieve. We report on those about corrective measures, sanctions, fines or 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 ensure that we properly consider whether to redact confidential, personally or commercially sensitive information when publishing details of specific cases. We also set our internal service performance measures to focus on impacts and outcomes rather than any prescribed sanction or regulatory activity levels.

What does this mean for a regulated entity?

As described above, we aim to respond swiftly and effectively to serious breaches of legislation that fall within our remit and when we do take enforcement action, we aim to be effective, proportionate, dissuasive, fair and consistent. There may be circumstances, such as in urgent or emergency situations, where you have to take decisions rapidly and there is less time to consider issues in detail, it can be particularly difficult to make sound judgements about whether to share information. The UK GDPR and the DPA 2018 do not prevent you from sharing personal data where it is appropriate to do so and our approach to regulatory action in these circumstances will be proportionate.

Further reading

Strategic plan [this document is to be updated in due course]

Data sharing: a code of practice | ICO

Assessing the outcomes of our regulatory actions

We review how effective our chosen regulatory activities are in achieving our desired outcomes. We will seek to identify clear objectives when we exercise our regulatory responsibilities so that we can review the impact of our actions against these objectives.

When we undertake any discretionary regulatory activity we will consider how best to evaluate its impact. As an organisation that is alert, effective and always learning we are open to feedback and are working to improve the quality of our outputs.

It is important that we review the outcome of our regulatory interventions, because it allows us to regulate more effectively in several ways:

- Most obviously, it allows us to learn from our experience by understanding what works and why, so that we can apply this in our future regulatory actions and prioritisation.
- It aids transparency for the public, organisations and others about our effectiveness in delivering our objectives.
- It provides an evidence base for demonstrating that our interventions are proportionate and allows us to support government in updating regulations to make them more effective.
- Finally, it helps us to demonstrate our net impact as a regulator, as we must assess the economic impact of regulation on businesses.

We are committed to assessing our outcomes and effectiveness in a number of ways, which vary based on the subject matter and regulatory actions we take. We:

- use intelligence analysis, horizon scanning and risk assessment methodologies to understand the changing information rights landscape, using this work to prioritise and focus future work;
- follow up, where appropriate, when we take regulatory action to assess ongoing compliance as well as assessing the work's impact. Where necessary, we may use other regulatory tools if our initial action does not achieve the desired outcome;
- debrief those involved in substantial operations, involving internal and external participants to understand how our action and messaging is received and its impact. We use this process to identify areas to improve within our ways of working; and
- seek to develop and make use of tools to quantify the impact of our highest priority and most significant work. Specifically, we look to see how effective our activity is in achieving our objectives.

More broadly, we are responsible for contributing to the Government's system of democratic accountability. We make information available to the public on the quality and productivity of our services, value for money, performance and progress on delivery. To support this, we publish annual reports of our activities on our website. These reports measure our performance against our key priorities which we publish in our strategic plans. The annual report includes key operational, financial and performance indicators. We are accountable to Parliament and report against agreed performance indicators to the Department for Culture, Media and Sport (DCMS) Select Committee.

Further reading

Business impact targets (BIT)

Our strategies and plans and annual reports

Our relationship with DCMS and our management agreement

Communication and co-operation

How do we communicate our regulatory activities?

We aim to be an effective, open and transparent regulator. Our approach is to be as open as we can although some of our duties and obligations may mean this is not always possible. When it is right to do so, we publicise the details of our regulatory work. This helps us achieve our strategic aims.

Publicity helps to raise confidence in, and awareness of, our work to promote good practice and deter those who might breach information rights legislation. However, we must be confident of the legality of – and public interest in – the information we publicise about our regulatory work and those we regulate. We must also make sure that publicising our work does not prejudice ongoing investigations or our future regulatory activity.

Our policy on communicating our regulatory enforcement activity sets out in detail how we make decisions about whether to publish or publicise information about our regulatory activity, which includes considering factors such as any financial market reporting obligations. The policy explains how we respond to requests for information about our work.

> **Further reading**
>
> Communicating our regulatory enforcement activity policy (CREAP)

How do we work with other regulators?

We often work with a range of other regulators and agencies to deliver our remit. This includes, but is not limited to:

- the National Cyber Security Centre, in our role as a NIS competent authority, and in the immediate response phase to cyber-attacks which lead to personal data breaches;
- other NIS competent authorities, such as the Civil Aviation Authority;
- law enforcement, including the National Crime Agency, in cases involving the theft or criminal misuse of personal data;
- sector, consumer and competition regulators, including the Financial Conduct Authority (FCA), The Office of Communications (Ofcom) and the Competition and Markets Authority (CMA) (through the Digital Regulation Cooperation Forum); and
- the Insolvency Service, in our work to recover penalties.

We share intelligence, threat analyses, insight and tactics with these organisations. We also refer relevant cases if 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 (eg minimising duplication of evidence gathering or information requests). We are at times required by law to consult about our regulatory conclusions, for instance with the National Archives when issuing a practice recommendation about a breach of the Code of Practice issued under section 46 of FOIA. We set out these arrangements in protocols and memoranda of understanding and publish them on our website.

Where necessary, we also do additional work with other regulators to support our regulatory action. For example, if a company seeks to avoid a financial penalty through complex liability structures or by dissolution, we pursue matters through winding-up orders or by referral to the Insolvency Service. We achieved success in obtaining director disqualifications and winding-up orders to disrupt those who repeatedly break the rules, and we are expanding our work in this area. If we find that a person or organisation profited from the misuse of data, then we can work alongside agencies who can confiscate money made from data misuse under the Proceeds of Crime Act.

We also work with other bodies in our regulatory activities for the UK digital economy. We have strong working relationships with the CMA, Ofcom and the FCA and, together with these partners, we formed the Digital Regulation Co-operation Forum (DRCF), a non-statutory body. Through the DRCF, we hope to develop this co-operation further. Its objectives include:

- collaboration between the three partners to reach a coherent regulatory approach to online and digital services;
- addressing emerging trends in digital markets; and
- jointly enhancing our regulatory capabilities and resources in this area.

In support of our fair approach to regulatory action, we share experiences with other regulatory bodies through our UK Regulator's Network (UKRN) membership. The UKRN brings together regulators from the UK's utility, financial and transport sectors for the benefit of consumers and the economy. This network gives us an opportunity to share knowledge and best practice, as well as to identify areas where a collaborative approach benefits both consumers and the economy. Our membership with networks like this supports our strategic goals and encourages strategic thinking with other bodies to promote learning, consistent guidance and standards.

> **Further reading**
>
> Working with other bodies
>
> ICO statement on joining the UKRN

Digital Regulation Co-operation Forum (DCRF)

How do we co-operate with data protection and information access regulators around the world?

To effectively protect the UK public's information rights, we need to co-operate and act internationally. The DPA 2018 allows us to position ourself internationally, as reflected in our international strategy, recognising the importance of engagement at a global level to support our role as UK regulator.

Section 120 of the DPA 2018 and the UK GDPR (Article 50) specifically requires us to engage with other countries and international organisations for the purpose of furthering international co-operation.

International co-operation on enforcement and formal regulatory interventions are a key part of the ICO's toolbox to uphold the UK public's data protection rights and hold organisations to account, allowing us to regulate in a modern, cross-border economy. Indeed, in today's world it's essential to be able to work with regulatory partners across jurisdictions, where data knows no borders and innovation has global, cross-regulatory implications. Such co-operation enables us to identify the most appropriate regulatory response, as well as share information to assist investigations, provide mutual assistance and secure appropriate regulatory outcomes.

We share intelligence, information, threat analyses, tactics, guidance and learning with the below groups. Where appropriate, we co-ordinate our investigative and evidence gathering activity with these partners; this is either jointly or individually, depending on the circumstances of the case. We may choose to collaborate internationally when two or more jurisdictions have a shared interest in the matter; for example, because an organisation's actions may affect members of the public in our respective countries, or because we see similar trends in the use of a particular technology.

A key example is our work as part of the Global Privacy Assembly (GPA). The ICO and the Information Commissioner have consistently been involved with the GPA on a number of levels. We addressed issues such as international enforcement co-operation and global frameworks and standards, both of which contributed to cross-border collaboration at a global level. We also worked on and sponsored resolutions to promote best practice and development relating to:

- AI development;
- the digital economy;
- digital citizen and consumer issues; and
- digital education.

A further way we foster international cooperation to support our UK regulatory role is through well-established working relationships. These relationships may also include the development of bilateral Memoranda of Understanding (MoUs) with other data protection and privacy authorities.

These MoUs establish a framework for cooperation and highlight how we can share information and expertise so that we can address either systemic issues (such as the privacy issues arising from emerging applications of technology) or to assess implications of a particular organisation's actions on the UK public, or both. The information we exchange most often relates to our regulatory approaches and, in some cases, the potential for joint investigations. We publish more information about these MoUs on our website.

We already have a significant international standing, being an active participant in the following key global data protection and information rights fora:

- **British, Irish and Islands' Data Protection Authorities network (BIIDPA)**

  BIIDPA is a small network dating back to the 1980s. It brings together data protection authorities from (often small) jurisdictions with shared data flows and common issues. As a member of BIIDPA, we support capacity building, help develop and influence common approaches and interpretations on key issues.

- **Common Thread Network (CTN)**

  We co-chair CTN, a forum which connects Commonwealth data protection and privacy regulators and supports countries that are developing national approaches. We use CTN as a platform to promote cross-border co-operation and build capacity by sharing knowledge on emerging trends, regulatory changes and best practices for effective data protection.

- **Conference of European Data Protection Authorities**

  A regional grouping of data protection authorities from member states of the EU and the Council of Europe (CoE). Our membership allows us to develop and maintain important regional relationships to support potential for future regulatory cooperation.

- **Council of Europe (CoE) Committee of Convention 108**

  The CoE is an international organisation founded in the wake of World War II to uphold human rights, democracy and the rule of law in Europe. We support the UK Government as the UK representative in the CoE, specifically in relation to the operation of Convention 108 (The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) and development of the modernised C108(+). We provide expert advice to protect and promote UK interests in CoE negotiations. Following the UK's withdrawal from the EU, Convention 108 represents the

UK's primary international legal commitment to robust, shared data protection standards.

- **Global Privacy Assembly (GPA)**

  The GPA is the premier global forum for data protection and privacy authorities with more than 130 members and observers worldwide. The ICO led the GPA from 2018 to 2021, which allowed us to influence debate and develop shared approaches at a global level on key emerging issues. These include data protection and accountability in AI development and within the digital economy, which supports our role as a regulator promoting innovation in the UK economy. We lead or are a member of a number of working groups, looking at issues such as:

  - the interoperability of global regimes;
  - facial recognition technology;
  - digital education; and
  - furthering international enforcement cooperation.

  In 2019, the International Enforcement Cooperation Working Group (IEWG) became a permanent GPA working group. As co-chair, we spearheaded its establishment as a forum for practical enforcement co-operation on live issues with a global impact on privacy. We use the IEWG as our principal gateway to drive timely joint enforcement activity on key and pressing issues of regulatory concern.

- **Global Privacy Enforcement Network (GPEN)**

  Since 2010, GPEN supported privacy authorities with cross-border enforcement of data protection and privacy laws. They do this through information exchange and unique activities such as global privacy compliance sweeps. The ICO sits on the GPEN committee, through which we build, maintain and strengthen valuable operational relationships with regulatory partners in several key jurisdictions.

- **International Conference of Information Commissioners (ICIC)**

  The ICIC is a global forum connecting member Information Commissioners, who are responsible for the protection and promotion of access to information laws. The ICIC's mission is to share knowledge and best practices, to build capacity, to help identify what is needed for global progress and to act as a collective voice in international forums. This is done to improve people's right to public information and their ability to hold public bodies to account. The ICO acted as chair of the ICIC from 2019 to 2021. During this time, we provided leadership in laying the foundations for the ICIC to function effectively, expand its global membership and promote its voice on important information rights issues. The ICIC continues to participate in key working groups related to strategic priorities, independent funding and collaboration projects with its

partner UNESCO (the United Nations Educational, Scientific and Cultural Organisation).

- **Organisation for Economic Co-operation and Development (OECD) Working Party on Data Governance and Privacy in the Digital Economy**

  Founded in 1961 to stimulate economic progress and world trade, the OECD is an inter-governmental economic organisation with 37 member countries. The DGP working party, chaired by our Deputy Commissioner for Regulatory Strategy, is a sub-committee to the Committee of Digital Economy Policy which itself reports to the OECD Council. We are well-placed to influence developing work on legally binding recommendations related to enhanced access and sharing of data, AI and discussions about the potential review of the OECD's privacy guidelines. The ICO's leading work on the Age Appropriate Design Code influenced the development of the revised OECD recommendation on children's privacy. We deliver this role in close co-ordination with the UK Government who represent the UK at the working party, to achieve outcomes that support UK policy intent.

- **Unsolicited Communications Enforcement Network (UCENet)**

  We sit on the executive committee of UCENet, which promotes international spam enforcement co-operation and addresses related issues such as online fraud and deception, phishing and dissemination of viruses. We actively engage in the network in the exchange of information and in order to develop international relationships in this area to aid our regulatory work.

Further reading

Our international work

Working with other bodies

Looking to the future

We will continue to be a flexible and responsive regulator, seeking innovative responses to new challenges as they arise. We aim to be responsive to the needs and concerns of the public using our risk-based approach to focus on issues which could cause the most harm. We continue to proactively monitor the information rights landscape, enabling us to respond quickly to new ideas and opportunities. We will also highlight where information rights can be strengthened. Working within the Regulators' Code, our focus is on compliance and using our enforcement powers proportionately and effectively to achieve the best results for the UK public.

Transparency is important to us and that is one of the reasons we are publishing this policy. This document reflects how we focus our efforts and resources to tackle breaches of the legislation we regulate and how we use our judgement to make difficult decisions.

Times are challenging and the ICO's response to the COVID-19 pandemic demonstrates we have the knowledge and skills to respond quickly and effectively to new challenges. We continue to build our capacity and evolve our strategies as new technologies and ideas around data and information rights develop. We are confident we possess the skills, knowledge and experience to continue to provide robust regulation of the UK's evolving information rights landscape.

We will keep this policy under review and will update it, as and when necessary, to reflect any amendments to the legislation which this policy covers. We will continue to develop what we do and to focus on improving our levels of service to the public and those we regulate.

Part B: The legislation we monitor and enforce

UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018)

What is the UK GDPR?

The UK GDPR is a regulation which explains how organisations should handle personal data. It also sets out the rights which people have over how organisations collect and use their data.

It came into force after the UK left the European Union, when the EU GDPR was incorporated into UK law through section 3 of the European Union (Withdrawal) Act 2018.

What is the DPA 2018?

The DPA 2018 sets out the framework for UK data protection law and sits alongside the UK GDPR. The ICO's responsibilities to monitor and enforce against the UK GDPR are set out in the DPA 2018.

What are our regulatory responsibilities under the UK GDPR and the DPA 2018?

We are responsible for monitoring the application of the UK GDPR (Article 51 (1)) and the DPA 2018.

When carrying out our responsibilities under the UK GDPR and the DPA 2018, we must consider the importance of securing an appropriate level of protection for personal data and take account of the interests of members of the public, organisations and others and matters of general public interest (section 2(2) DPA 2018).

We must publish and produce for Parliament an annual report on our work. We may also produce other specific reports on our work for Parliament (under section 139 DPA 2018).

The ICO has a responsibility to:

- make sure organisations properly apply the UK GDPR and DPA 2018, and take enforcement action if we decide they do not;
- raise public awareness and understanding of the risks, rules, safeguards and rights in relation to processing personal data, especially with children's data;
- provide advice to Parliament, the government and other institutions and bodies about the public's data rights and the processing of personal data under UK GDPR and DPA 2018;

- handle complaints from the public about how organisations use their data and investigate as necessary;
- conduct investigations on how organisations apply the UK GDPR and DPA 2018; and
- monitor relevant developments which impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices; and
- monitor and enforce Part 3 (law enforcement processing) and Part 4 (intelligence services processing) of the DPA 2018 and carry out the functions as set out in Schedule 13 of the DPA 2018 in respect of those Parts.

What regulatory action can we take?

If we think an organisation or person breached the UK GDPR or DPA 2018 then it's our responsibility to provide formal advice, investigate or take corrective action to ensure organisations handle personal data appropriately.

Under these responsibilities we have various powers (listed in Article 58 UK GDPR and Part 6 of the DPA 2018), including the power to:

- serve an information notice to order an organisation to provide us with any information we need to help us understand whether they breached data protection law (under section 142 DPA 2018);
- carry out investigations or data protection audits to help us understand how organisations use and store data by serving an assessment notice (under section 146 DPA 2018);
- notify the organisation of alleged breaches of the UK GDPR or DPA 2018;
- access any premises that an organisation uses, including any data processing equipment and means;
- warn an organisation if we think that their planned processing activity is likely to breach the UK GDPR or DPA 2018;
- reprimand an organisation if they breach the UK GDPR or DPA 2018 with their data processing activities;
- issue an enforcement notice (under section 149 DPA 2018) to:
    - order an organisation to comply with a member of the public's requests to exercise their rights under the UK GDPR or DPA 2018;
    - order an organisation to change the way they handle data so they comply with the UK GDPR or DPA 2018;
    - order an organisation to tell a member of the public about a personal data breach;
    - set temporary or defined limits on data processing (including a ban);

    - order an organisation to correct inaccuracies in personal data, erase personal data or restrict the way they process data;
    - withdraw a certification of compliance with the provisions of UK GDPR or DPA 2018; and
    - order the suspension of data flows to a recipient in a third country or to an international organisation.
- impose a financial penalty (by giving a penalty notice under section 155 DPA 2018);
- give advice to an organisation, Parliament or National Assembly in accordance with the prior consultation procedure (referred to in Article 36 UK GDPR);
- give Opinions, on our own initiative or on request, to Parliament, government or to other institutions and bodies as well as to the public on any issues related to data protection;
- issue an Opinion and approve draft codes of conduct (as required by Article 40(5) UK GDPR);
- issue certifications and approve criteria of certification (in accordance with Article 42(5) UK GDPR);
- accredit certification bodies (as required by Article 43 UK GDPR);
- adopt standard data protection clauses (referred to in Article 28(8) and in point (d) of Article 46(2) UK GDPR);
- authorise contractual clauses (referred to in point (a) of Article 46(3) UK GDPR);
- authorise administrative arrangements referred to in point (b) of Article 46(3) UK GDPR;
- approve binding corporate rules (as required by Article 47 UK GDPR); and
- obtain, from an organisation, access to all personal data and all information necessary for the performance of our tasks.

Under section 197 DPA 2018, we can bring cases to court if we believe a member of the public or organisation committed an offence under the DPA 2018 (except in Scotland, where the Scottish Crown Office and Procurator Fiscal brings prosecutions).

Further reading

Guide to Data Protection

Guidance on codes of conduct

Guidance on certification

Freedom of Information Act 2000 (FOIA)

What is FOIA?

FOIA provides the public with access to certain information that public authorities in England, Wales and Northern Ireland hold, and UK-wide public authorities based in Scotland. Scotland's own Freedom of Information (Scotland) Act 2002, regulated by the Scottish Information Commissioner, covers information that Scottish public authorities hold.

FOIA requires public authorities to publish certain information about their activities, and members of the public can request further information from them.

What are our regulatory responsibilities under this Act?

Section 47 FOIA lists our general responsibilities which include:

- promoting good practice by public authorities and to perform our obligations so as encourage public authorities to follow FOIA requirements and the associated codes of practice;
- sharing information with the public about how FOIA works, what good practice looks like and what the ICO's role is in relation to FOIA;
- giving advice to the public and public authorities about FOIA; and
- assessing whether a public authority (with their consent) is following good practice.

What regulatory action can we take?

If we believe a public authority is not acting appropriately regarding their duties under FOIA and its associated codes of practice, then we can (under section 48 FOIA) make formal recommendations explaining what they need to do to meet their obligations. Where such a recommendation relates to the section 46 Code of Practice about good record keeping and compliance with the relevant Public Records Act, we will consult with The National Archives.

Anyone can ask us to decide whether a public authority dealt with a particular request for information in line with FOIA. If we decide that they did not, we can issue a decision notice (in compliance with section 50 FOIA) which tells the public authority what they must do to comply with FOIA.

If we are not sure whether a public authority is complying with FOIA or we need further information, then we can issue an information notice (section 51 FOIA). This requires the public authority to provide information to us which helps us to decide.

If we decide that a public authority is not complying with FOIA, then we can issue an enforcement notice. This can make the public authority comply with any of the requirements of Part I of FOIA (section 52 FOIA).

If a public authority does not comply with a notice we issue, then we can write to the court to make it aware of this (section 54 FOIA). This could result in the public authority being held in contempt of court.

If a public authority fails or is failing to comply with FOIA, we can ask the court for a warrant to:

- enter and search premises;
- inspect and seize documents or other material; and
- inspect, examine, operate and test any equipment which may hold information (section 55 and Schedule 3 FOIA).

Under section 77 FOIA we may decide to take a public authority (or any person who is employed by, an officer of or subject to the direction of the public authority) to court for an offence of altering records with intent to prevent disclosure (except for offences committed in Scotland, which we would refer to the Procurator Fiscal).

Further reading

Guide to freedom of information

Re-use of Public Sector Information regulations 2015 (RPSI)

What are the RPSI regulations?

The RPSI regulations set out how Public Sector Bodies (PSBs) should make public sector information available and about how others can re-use it.

Public sector information is information a PSB produces as part of their core role and functions. Regulation 3 lists PSBs covered by the RPSI.

RPSI only applies to accessible information, ie information that is not exempt from disclosure under its relevant legislation and that does not contain third-party intellectual property rights.

A person can request permission to re-use public sector information, but only if that use is different from its original use.

A PSB, when permitting re-use, should make the information available in the format in which they hold it at the date of the request. Where possible, the information should be in an open and machine-readable format.

Where a PSB refuses permission for a person to re-use public sector information or if they apply restrictions on the re-use, they should request an internal review. If the requester remains dissatisfied after that review, they can ask us to investigate the matter.

What are our regulatory responsibilities under these regulations?

Our role is to deal with complaints against those PSBs about how they handle matters regarding re-use requests that they refuse.

What regulatory action can we take?

Our decision-making and investigatory responsibilities in RPSI come from the equivalent provisions in FOIA. An ICO investigation could conclude with a decision, recommendation notice or a finding that the RPSI is not applicable.

> **Further reading**
>
> Guide to RPSI

Environmental Information Regulations 2004 (EIR)

What are the EIR?

The EIR provide public access to certain environmental information that public authorities in England, Northern Ireland and Wales hold. Scottish public authorities are subject to the Environmental Information (Scotland) Regulations 2004. The Scottish Information Commissioner regulates these.

What are our regulatory responsibilities under these regulations?

Our general responsibilities under section 47 of FOIA (see above) also apply to the EIR.

What regulatory action can we take?

Our responsibilities under FOIA (see above) also apply to the EIR.

> **Further reading**
>
> Guide to the Environmental Information Regulations

INSPIRE regulations 2009

What are the INSPIRE regulations?

The Environmental Protection Public Sector Information regulations 2009 are also known as the INSPIRE regulations. They cover spatial data, which is any data with a direct or indirect reference to a specific location or geographical area.

The regulations apply to all public authorities in England, Wales and Northern Ireland (as defined by the EIR) that hold one or more spatial data sets. They also apply to any organisation or person holding spatial data on behalf of a public authority. Complementary INSPIRE regulations apply in Scotland and the Scottish Information Commissioner enforces these.

What are our regulatory responsibilities under these regulations?

We have limited responsibilities (set out in section 9) to consider complaints under the INSPIRE regulations.

We can consider complaints that public authorities are wrongly withholding information because it contains personal data.

We can also consider complaints where public authorities decide to share or withhold information. We can assess whether a public authority fully considered if their decision is in the public interest.

What regulatory action can we take?

Regulation 11 imports the enforcement provisions of FOIA into the INSPIRE regulations 2009.

> **Further reading**
>
> Guide to the INSPIRE Regulations

Privacy and Electronic Communications Regulations (PECR)

What is PECR?

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) sit alongside the DPA 2018 and the UK GDPR. PECR give people specific privacy rights in relation to electronic communications like emails, automated calls, cookies and text messages.

What are our regulatory responsibilities under this regulation?

We aim to help organisations comply with PECR and promote good practice by offering advice and guidance. We will take enforcement action against organisations that ignore their obligations.

What regulatory action can we take?

Under Regulation 5 of PECR we may carry out audits to ensure compliance with the requirements of PECR in respect of security measures taken to safeguard the security of the service (Regulation 5(1)), and the notification of personal data breaches (Regulation 5A). We may also require service providers to notify subscribers or users of a personal data breach. If a service provider fails to comply with the notification requirements of Regulation 5A, we may issue a fixed penalty notice in respect of that failure.

Under Regulation 31A of PECR, we may serve a third-party information notice to require a communications provider to provide information to us.

Further, under Regulation 31(1) of PECR, the provisions of Part V and sections 55A to 55E (dealing with monetary penalties) and Schedules 6 (Appeal proceedings) and 9 (Powers of entry and inspection) of the DPA 1998 are extended for the purposes of PECR (subject to the modifications set out in Schedule 1 of PECR). These provisions of the DPA 1998 remain in force for the purposes of PECR, even with the introduction of the DPA 2018.

> **Further reading**
>
> Guide to Privacy and Electronic Communications Regulations

Network and Information Systems regulations 2018 (NIS)

What are the NIS regulations?

The Network and Information Systems regulations 2018 (NIS) aim to establish a common level of security for IT network and information systems.

We are the designated competent authority for relevant digital service providers (RDSPs) who provide online marketplaces, cloud computing services or online search engines in the UK.

What are our regulatory responsibilities under this regulation?

Under regulation 3(4) NIS we must:

- review the application of the NIS;
- prepare and publish guidance; and
- consult and co-operate with other relevant organisations (eg law enforcement) to fulfil the NIS requirements.

As the designated competent authority for RDSPs, we must act when an incident notification provides us with evidence that a digital service provider does not meet the NIS requirements.

Regulation 12(8) NIS says we must share any incident notification we receive from an RDSP with the relevant computer security incident response team (CSIRT), which in the UK is the NCSC.

Regulation 12(15) NIS says we must provide an annual report to the NCSC, identifying the number and nature of notified incidents.

Regulation 13 NIS says, we may give information and assistance to, and otherwise co-operate with, a public authority in the EU if the Information Commissioner considers that to do so would be in the interests of effective supervision of digital service providers (whether inside or outside the United Kingdom), including in the event of an incident notified under regulation 12(3).

RDSPs need to register with the ICO. Under Regulation 14(1) NIS we must maintain a list of all registered RDSPs.

Regulation 12(12) NIS says we may inform the public about an incident, or tell the RDSP responsible to do so, if it is in the public interest or if it is necessary to prevent or manage the incident. Before informing the public, we must consult the NCSC and the RDSP (regulation 12(13) NIS).

Regulation 12(14) NIS says that, in certain circumstances, we may inform the public about an incident affecting digital services in an EU member state.

What regulatory action can we take?

We have the power (regulation 15(3) NIS) to issue an information notice to an RDSP and ask them to provide certain information. This could help us assess the security of the network and information systems and the implementation of their security policies.

Under Regulation 16(2) NIS, if we receive evidence that an RDSP is not meeting their requirements, we can conduct an inspection (or appoint a person, either directly or through the RDSP, to conduct an inspection on our behalf) to assess if a RDSP is fulfilling their requirements.

Regulation 17(2) NIS says we can issue an enforcement notice to an RDSP if we believe that they failed to comply with certain duties and requirements (eg a failure to notify an incident under regulation 12(3) NIS). Regulation 17 (2A) further states that, before serving an enforcement notice under paragraph 17 (2), we must inform the RDSP of:

- the alleged failure; and
- how and by when they may make representations in relation to the alleged failure and any related matters.

Under regulation 18(2) NIS, we may serve a notice of intention to impose a penalty on a RDSP. We can do this if we believe that the RDSP failed to comply with a duty from regulation 17(2) or the duty set out in regulation 17(3A), and consider that, taking into account the facts and circumstances of the case, it warrants a penalty. The notice of intention to impose a penalty must specify the following:

- the reasons for imposing a penalty;
- the penalty amount and how to pay;
- the date of the notice;
- the period within which a penalty needs to be paid, if serving a penalty notice;
- that the payment of a penalty under a penalty notice (if any) is separate to any enforcement notice requirements; and
- how and when they may make representations about the content of the notice of intention to impose a penalty and any related matters.

Under regulation 18(3B) we may, after considering any representations the RDSP submits in accordance with paragraph (3)(f), serve a penalty notice on the RDSP. This includes a final penalty decision if, taking into account the facts and circumstances of the case, we believe that it warrants a penalty..

Under regulation 18(3D), a penalty notice must:

- be in writing to the RDSP;

- include reasons for the final penalty decision;
- require the RDSP to pay:
    - the penalty specified in the notice of intention to impose a penalty; or
    - an appropriate penalty, in the light of any representations the RDSP makes and any steps they take to rectify the failure or to do any actions required by an enforcement notice under regulation 17(3);
- specify the period within which the RDSP must pay the penalty ("the payment period") and when the payment period begins;
- provide details of the appeal process under regulation 19A; and
- specify the consequences of failing to make payment within the payment period.

Under regulation 19A NIS, the RDSP has a right to appeal to the First-tier Tribunal against the decision to serve an enforcement notice or a penalty notice.

Under regulation A20 NIS, where we believe that a RDSP failed to comply with an enforcement notice's requirements, as mandated by regulation 17(3A), we may begin civil proceedings against the RSDP to obtain an injunction to enforce the duty or for any other appropriate remedy or relief. However, we may not bring or continue proceedings under this regulation if an RDSP appealed under regulation 19A and the Tribunal granted a suspension, for as long as that suspension is in effect.

Under regulation 23(1) NIS, before we take any action under regulations 17(2) or 18(3B), we must consider whether, on the facts and circumstances of the case, it would be reasonable and proportionate. Further, under regulation 23(2) NIS, we must also consider the various matters listed including, any representations the RDSP makes about the contravention and any steps they take to rectify the contravention.

> **Further reading**
> The Guide to NIS

Electronic Identification and Trust Services for Electronic Transactions (UK eIDAS)

What are the UK eIDAS regulations?

Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (EU eIDAS Regulation) is a European regulation. It is incorporated into UK law by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc) (EU Exit) regulations 2019.

There are also some specific provisions on their effect, supervision and enforcement in the UK, which are set out in the Electronic Identification and Trust Services for Electronic Transactions regulations (2016) (the UK eIDAS regulations).

These eIDAS regulations aim to enhance trust in electronic transactions between businesses, citizens and public authorities by providing a common legal framework and consistent rules on trust services across the UK. The regulations also recognise the legal effect of trust services meeting qualified status under the EU's equivalent legislation.

What are our regulatory responsibilities under these regulations?

We are the supervisory body and have the responsibilities set out in the eIDAS regulations, including to:

- verify and supervise qualified UK trust service providers and to ensure that they meet the requirements of the UK eIDAS regulations; and
- act, if necessary, in relation to non-qualified UK trust service providers where they allegedly do not meet the requirements of the UK eIDAS Regulations.

What regulatory action can we take?

Our powers include the ability to:

- carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers;
- withdraw qualified status from qualified trust service providers;
- inform the public, or require the trust service provider to do so, where we determine that disclosure of the breach of security or loss of integrity is in the public interest;
- bring criminal prosecutions for offences under these regulations; and

- take enforcement action, including issuing:
    - fixed monetary penalties;
    - information notices;
    - assessment notices; and
    - enforcement notices.

Further reading

Guide to eIDAS

The EU eIDAS Regulation: Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market

The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019

The UK eIDAS Regulations: The Electronic Identification and Trust Services for Electronic Transactions Regulations (2016)

Enterprise Act 2002

What is the Enterprise Act?

The Enterprise Act made a number of significant reforms to UK competition law and consumer law enforcement.

Part 8 of the Enterprise Act deals with provisions for the enforcement of consumer protection legislation and identifies two types of breach which trigger the Part 8 enforcement powers. They are:

- Domestic infringements: which are infringements of particular UK enactments or of contractual or tortious duties, in each case if they occur in the course of a business and in relation to goods or services supplied or sought to be supplied:
    - to or for a person in the UK; or
    - by a person with a place of business in the UK; and
- Schedule 13 infringements: which are infringements of the legislation listed in schedule 13 of the Enterprise Act.

To trigger those powers, in both cases the infringement must harm the collective interest of consumers.

What are our regulatory responsibilities under this Act?

Along with other UK authorities, we have powers under Part 8 of the Enterprise Act. They are both as a "designated enforcer", in relation to domestic and schedule 13 infringements, and as a "schedule 13 enforcer", which gives us additional powers in relation to schedule 13 infringements.

What regulatory action can we take?

As a designated enforcer, we can make an application for an enforcement order in respect of an infringement requiring, for example, a person to cease conduct harmful to consumers.

Further, as a schedule 13 enforcer, we can:

- enter premises with or without a warrant (upon meeting certain conditions);
- observe the carrying on of business;
- purchase and inspect products;
- require the production of documents;
- inspect and take copies of evidence or records;
- break open any container or access any electronic device which may store or be able to access information;

- require assistance from any person on the premises; and
- seize and detain goods and documents.

Further reading

Enterprise Act 2002

Consumer Rights Act 2015 (legislation.gov.uk)

Investigatory Powers Act 2016 (IPA)

What is the IPA?

The Investigatory Powers Act 2016 (IPA) sets out the electronic surveillance powers of the UK intelligence community and police. It also provides safeguards on the exercise of those powers.

What are our regulatory responsibilities under this Act?

Under the Act, the Secretary of State may ask telecommunications providers to retain relevant communications data. The ICO has a responsibility (section 244 IPA) to audit this data to make sure telecommunications companies are safely storing this information and disposing of it securely. The ICO audits these telecommunications companies on a rolling basis and, where appropriate, makes recommendations on how to mitigate any risks of non-compliance with Part 4 of IPA.

What regulatory action can we take?

IPA does not provide the ICO with any enforcement powers. However, as retained data is almost always personal data, we can use our enforcement powers under the DPA 2018 to help us carry out our regulatory responsibilities.

This could include:

- serving an information notice and ordering a telecommunications provider to provide us with any information we need to help us understand whether they breached data protection law (under section 142 DPA 2018);
- serving an assessment notice and accessing any premises used, including access to any data processing equipment and means (under section 146 DPA 2018);
- issuing a warning if we think that their planned processing activity is likely to breach the UK GDPR;
- issuing a reprimand where the provider breaches the UK GDPR through their data processing activities;
- issuing an enforcement notice (under section 149 DPA 2018) to order a provider to change the way they handle data to comply with the UK GDPR; and
- imposing a financial penalty (by giving a penalty notice under section 155 DPA 2018).

Further reading

Investigatory Powers Act 2016