

# ICO25 – Our regulatory approach

7 November 2022



# Contents

Foreword .....	3
About this document .....	4
Which legislation does this explanation cover? .....	5
How we help you comply with the legislation we monitor and enforce ....	7
Our legal responsibilities.....	10
How do we meet our obligations to support economic growth?.....	12
What other ICO policies and strategies do we have? .....	13
How do we make regulatory policy? .....	13
Our approach to our regulatory responsibilities .....	14
How do we prioritise our work? .....	14
How do we approach our regulatory responsibilities?.....	15
What does this mean for regulated entities and their staff? .....	15
Assessing the outcomes of our regulatory actions .....	17
Communication and co-operation .....	19
How do we communicate our regulatory activities? .....	19
How do we work with other regulators?.....	19
How do we co-operate with data protection and information access regulators around the world? .....	21
Looking to the future.....	25
The legislation we monitor and enforce .....	26
UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).....	26
Freedom of Information Act 2000 (FOIA) .....	29
Re-use of Public Sector Information Regulations 2015 (RPSI) .....	30
Environmental Information Regulations 2004 (EIR) .....	31
INSPIRE Regulations 2009.....	32
Privacy and Electronic Communications Regulations (PECR).....	32
Network and Information Systems regulations 2018 (NIS) .....	33
Electronic Identification and Trust Services for Electronic Transactions (eIDAS) .....	36
Enterprise Act 2002.....	37
Investigatory Powers Act 2016 (IPA) .....	39

## Foreword

Our [new strategic plan – ICO25](#) was published in July 2022. It describes our shift in approach and sets out:

- why our work is important;
- what we want to be known for and by whom; and
- how we intend to achieve this by 2025.

The environment we work in is complex, fast-moving and ever-changing. ICO25 helps us to understand and describe our priorities, enabling us to make informed choices about the action we take and the interventions we make. Our extensive stakeholder consultation and the responsibilities we have been given by Parliament have informed our approach.

This document explains how we will implement the ICO25 plan in our regulatory enforcement work and the current Regulatory action policy.

Many potential breaches of the legislation we regulate come to our attention on a daily basis. One of our key tasks is to prioritise our resources to ensure we take the most effective action and achieve the most impactful outcomes possible.

We recognise that often organisations are trying to do the right thing and may simply require guidance or clarification, rather than a sanction. We will not hesitate to take steps to protect people from the unscrupulous who wish to cause harm, or those who are reckless and seek to avoid their responsibilities. However, we will recognise where organisations have tried to do the right thing. For example, by taking advice, considering their information arrangements carefully, bringing in support when needed, and engaging openly with us as regulator.

This document explains how we will do this.

## About this document

The mission of the Information Commissioner's Office (ICO) is to uphold information rights for the UK public in the digital age. In accordance with ICO25, we want to be open and transparent about how we do this and how we work.

The legislation that governs our work requires us to produce statutory guidance on how we exercise our formal data protection powers to:

- require information (information notices);
- assess compliance (assessment notices);
- require an organisation to take steps to return them to compliance (enforcement notices); and
- levy financial penalties for non-compliance (monetary penalty notices).

Information about how the ICO exercises these formal powers is set out in our [Regulatory action policy](#) (pdf).

In the light of ICO25, we also want to be more open and transparent about the 'when' and 'why' of regulatory action, as well as the 'how'. We have written this document to explain how we plan to exercise our powers in the context of ICO25. We know from listening to our stakeholders that this is valuable and important to people.

The purpose of this document is to provide clarity to those we regulate and the public about our approach to selecting, prioritising and taking regulatory action. By regulatory action, we mean any action we decide to take in exercising our powers under the legislation we are responsible for. This includes giving opinions or advice, writing guidance, carrying out audits or assessments, taking enforcement action, issuing warnings or reprimands, and launching criminal prosecutions.

The first part of the document sets out our strategic approach and explains how we:

- promote best practice and empower organisations to use information responsibly;
- enable people to exercise their rights effectively and how we help ensure compliance;
- approach our regulatory responsibilities and prioritise the different calls on our resources to achieve the greatest impact;
- assess the outcomes of our regulatory action; and
- work with other regulators and reflect this in our decisions.

The second part summarises the individual pieces of legislation we are responsible for and provides examples of the specific regulatory action we can

take for each. This is not a comprehensive description of the legislation, rather it is provided to assist in identifying the scope of our regulatory remit.

Like all regulators and law enforcement agencies in the UK, our 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, most of our funding comes from the data protection fee, in the main paid by hundreds of thousands of small businesses in the UK.

Using the resources at our disposal, our approach aims to create an environment that protects people, provides a level playing field for businesses, and supports access to information.

We want to ensure that businesses, charities and public services can operate effectively in the digital age and are able to innovate. At the same time, we want to help organisations use, hold and share information in a transparent and accountable way. Establishing public trust and confidence in the way information is used is important in empowering people to participate in the digital economy.

We take a risk-based approach to regulatory action. This involves working with organisations and people that may fail to meet their obligations under the laws we regulate or who may need support or guidance to comply and innovate. Our focus is usually on areas of high risk where non-compliance could do the most harm.

We are as robust as we need to be in upholding the law, while ensuring that commercial businesses and public services are not worried that we may impose disproportionate sanctions for non-compliance. 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 people.

## Which legislation does this explanation 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 (RPSI);
- 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**

[ICO25 strategic plan](#)

[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 to empower people to exercise their rights and enable organisations to get things right when using, handling, sharing and storing information, including personal data. To support this, we:

- promote good practice;
- provide advice, tools and guidance; and
- provide authorisations and assurance.

We use our formal enforcement actions when necessary to protect people and prevent harm. This includes imposing penalties where appropriate. However, our experience is that most businesses and organisations want to do the right thing for customers and service users but sometimes need a steer or guide from us, as regulator, about what they need to think about or do.

For the public sector, we [have set out a distinct approach](#) that involves trialling over a two-year period the greater use of our discretion to reduce the impact of fines on the public. This is because a public sector fine often also impacts the victims of the breach, by reducing budgets for vital services. To support this approach, we will work proactively with senior leaders in the public sector to encourage compliance, prevent harms before they occur, and learn lessons when things have gone wrong. In practice, this means that for the public sector we will increase the use of public reprimands and enforcement notices, only issuing fines in the most egregious cases.

We are also working with the UK Government to establish a senior network of officials responsible for working with us to achieve better compliance with the law across Whitehall. We aim to replicate this across the other nations and key parts of the public sector where we think such strategic oversight would help.

We provide a number of other services to help people and organisations 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 guidance covers a wide range of topics including how to correctly handle information requests, people's information rights, how artificial intelligence should interact with personal data, and how organisations should process the most sensitive information.
- We provide advice explaining how organisations can better comply with the law. We publish common themes on our website so others can readily find advice and our position on specific compliance issues.

- We attend and host events and conferences to raise awareness of our work and the legislation we regulate. 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, case studies and expectations documents to raise awareness and promote information rights on specific issues involving information.
- We share our own staff training, guidance and manuals wherever possible; helping provide certainty about how we will consider specific circumstances or issues.
- We produce blogs, newsletters, webinars and use social media to raise awareness about our views on specific issues or concerns and to promote information rights.
- We publish decision notices about access to information appeals we have considered so public bodies can better understand how to handle the requests they receive. We are making this system searchable so that public authorities can apply our previous decisions to their live cases with greater certainty.
- We also use our decision notices, and where needed practice recommendations, 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 sized enterprises (SMEs), 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. We have also advised on DPIAs relating to COVID-19.
- We get key messages out quickly and effectively, and coordinate our work with key stakeholders.
- We work with trade organisations and sector bodies to provide sector specific guidance, advice, checklists and tools, either directly or through their own outreach programmes or sector helplines.
- We help organisations to test new and innovative data protection concepts in a safe environment through our regulatory sandbox. We've completed a diverse range of projects, which include supporting the higher education sector in developing new data-based tools to intervene and support student mental health. We have also supported the NHS in its response to COVID-19 and the development of a central mechanism to allow people to get



involved with researchers undertaking vaccine trials.

- We intervene to assist the courts with novel or contentious information rights cases to help clarify the law and provide certainty for regulated organisations.
- We collaborate with other regulators on initiatives that bring about innovation, including through our involvement with the Digital Regulation Co-operation Forum (DRCF). Our 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 practice in their own procedures when supporting business innovation.
- We investigate key issues of concern to people and produce reports that set out our findings, share learning and make recommendations about improving practice in the future. These reports provide important advice for organisations about how they can use information appropriately. For example, we investigated and reported on the way the police use the information 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; investigated the way credit reference agencies use personal data for marketing; and reported on the use of private correspondence channels by Ministers and others working at the Department of Health and Social Care (DHSC).

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

As a public authority, we have obligations and commitments that guide our regulatory activities and our work with other regulators as part of the UK's broad framework of regulation. Meeting these commitments ensures we are a responsible regulator that treats people fairly and with respect. As part of this, we work with our colleague regulators within the UK Regulators' Network (UKRN), as well as the Digital Regulation Co-operation Forum (DRCF) and the Regulatory Initiatives Forum to provide a co-ordinated and consistent approach.

- **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 only take regulatory action when we need to and ensure any action we do take is proportionate.

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

The Small Business, Enterprise and Employment Act 2015 and the Enterprise Act 2016 require regulators, including the ICO, to assess and report on 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 of the 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**

[UK’s Regulators Network](#)

[DRCF](#)

[Regulatory Initiatives Forum](#)

[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, effective and lawful. We achieve this in a range of ways.

When exercising our regulatory responsibilities, we consider how we can support, empower 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 compliance.

We are committed to developing the knowledge and understanding of our staff about those we regulate and enabling them to choose proportionate and effective approaches to regulation. We seek to maximise our impact, for example by taking action where we consider the risks and harms to be the greatest. However, we recognise the importance of understanding the impact of our actions to ensure that they are proportionate.

We offer clear, practical guidance and advice to organisations, explaining and helping them to meet their legal obligations. This serves to support innovation and economic growth. We provide 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 services support organisations' innovation in the use of information, while our grants programme encouraged innovation in privacy more generally.

We aim to provide appropriate, fair and straightforward ways for people 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.

### **Further reading**

[ICO Regulatory Policy Methodology](#)

[ICO SME Service Hub](#)

[ICO Innovation Services](#)

[ICO Regulatory Sandbox](#)

[ICO Grants programme \(ended\)](#)

## What other ICO policies and strategies do we have?

This document sits alongside our other policies, guidance and strategies (available at the link further below), that 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 includes deciding how to balance trade-offs between competing priorities, how to interpret legal provisions, and how to identify the challenges and opportunities of emerging technologies and business models.

It is important that we, as the regulator, are able to act impartially and independently because the government is also subject to information rights law. 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 are also developing a range of interventions to ensure that we have the right professional development opportunities and career paths in place.

### **Further reading**

[ICO25 strategic plan](#)

[ICO policies and procedures](#)

---

# Our approach to our regulatory responsibilities

## How do we prioritise our work?

We have finite resources and we are unable to look into every matter raised with us. We therefore need to focus on those issues posing the greatest risk of harm and keep this under review. We have a prioritisation framework that enables us to make the best use of our resources and achieve the greatest impact for the benefit of organisations throughout the UK and for the UK public more widely. This framework draws lessons from similar models in use by other UK regulators, and is aligned to the UK regulatory approach and Regulators' Code.

We consider each case on its merits and the risks or opportunities it presents. The prioritisation framework takes account of several factors, including:

- the likely impact of our actions, including considering the risks, harm and opportunities to improve compliance;
- alignment with our strategic priorities, including considering whether we are best placed to act or should work in collaboration with others (for example a sector regulator);
- the likelihood of successful regulatory outcomes consistent with achieving our aims; and
- the resources we will require to achieve those outcomes.

We balance these considerations against the risks of harm (perceived and evidenced). This involves assessing the:

- evidence available of that harm;
- degree of public concern;
- likelihood of success of any intervention; and
- legal, financial and reputational risks to the ICO.

We consider these issues in the round and on a case-by-case basis, taking account of the available evidence. We exercise judgement where necessary and take into account 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;
- consumer research, such as our annual 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 publishing a formal opinion, warning or reprimand. When we take enforcement action, we aim to be effective, proportionate, dissuasive, fair, and consistent. Our statutory guidance sets out the situations when we are likely to exercise our compulsory powers under the data protection legislation.

In general, when deciding whether and how to respond to information rights breaches, we consider each case individually and consider all relevant factors.

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. We keep organisations updated at regular intervals about the action we are taking and what likely conclusions we might reach.

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, any relevant learning for the sector, and the outcomes we achieve. As part of this, we report on corrective measures, sanctions, fines, enforcement notices or orders, fixed penalty notices, and criminal prosecutions. We may also publish case study examples to illustrate good practice or learning.

We consider whether to redact confidential, personally or commercially sensitive information when we publish details of specific cases. We also focus our performance measures on impacts and outcomes, rather than any prescribed sanction or regulatory activity levels.

## What does this mean for regulated entities and their staff?

We aim to respond swiftly and effectively to serious breaches of legislation that fall within our remit. When we do take enforcement action, we aim to be effective, proportionate, dissuasive, fair, and consistent.

We know that there may be circumstances where organisations have to take decisions rapidly under pressure and there may be less time to consider compliance issues in detail. For example, in urgent or emergency situations. We acknowledge that in these circumstances it can be difficult to make sound judgements about whether to share information or take specific actions with confidence.

We have heard that some staff within organisations do not take safeguarding action out of fear of being investigated or penalised by the ICO. However, the UK GDPR and the DPA 2018 does not prevent sharing personal data where it is appropriate to do so, or from taking steps to prevent harm. Our approach to regulatory action is proportionate and reflects the context of decisions being taken in difficult circumstances. Where information has been shared or steps have been taken in good faith to safeguard life, protect children or prevent harm, we will take this into account. In most cases it will mean we are unlikely to take enforcement action.

It also means that when selecting the right regulatory response to an incident or possible breach, we will consider carefully and recognise steps that an organisation has taken to comply with its obligations. This includes the advice it may have taken on measures to avoid a security breach. For example, whether it has sought advice from a professional recognised by the UK Cyber Security Council, the National Cyber Security Centre, or other equivalent organisation. As well as the practical steps it has implemented (such as obtaining certification through the government-backed Cyber Essentials scheme or by complying with another similar code or certification scheme).

For public sector organisations, our approach also means that any financial penalty may be reduced or replaced by a public reprimand. This is in recognition of the impact that paying a financial penalty may have on the funds available for publicly funded organisations to provide frontline services. It also recognises that for many public sector organisations, the publication of our investigatory findings may itself act as an effective deterrent. This reflects the approach agreed with public sector leaders to place greater focus on improvements to ensure information rights are upheld, including lessons learned from the incidents we investigate. We will keep this approach under review to see how effective it is at encouraging good compliance.

### **Further reading**

[ICO25 strategic plan](#)

[Data sharing: a code of practice | ICO](#)



## Assessing the outcomes of our regulatory actions

We seek to identify clear objectives when we exercise our regulatory responsibilities so that we can review the impact of our actions against them. When we undertake any regulatory action, we consider how best to evaluate its impact as part of our planning. We will report on this impact in our annual regulatory reports and economic impact assessments.

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 and legislation to make them more effective.
- It helps us to demonstrate our net impact as a regulator, including by assessing the economic impact on businesses of the regulatory action we take under our statutory duties.

We are committed to assessing our outcomes and effectiveness in a number of ways. These 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.
- We follow up, where appropriate, when we take regulatory action to assess ongoing compliance as well as assessing our work's impact. Where necessary, we may use other regulatory tools if our initial action does not achieve the desired outcome.
- We 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 our work.
- We seek to develop and make use of tools to quantify the impact of our highest priority and most significant work. In particular, 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 Digital, 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 and 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 (NCSC), in our role as a NIS competent authority and in the immediate response phase to cyber-attacks which lead to personal data breaches under data protection legislation. When deciding on our regulatory response to a personal data breach we will recognise the degree to which organisations have engaged with the NCSC and implemented its advice.
- Other NIS competent authorities, such as the Civil Aviation Authority, where we will consider the degree to which organisations have followed relevant sector standards governing information.
- Law enforcement, including the National Crime Agency, in cases involving the theft or criminal misuse of personal data.
- Sector, consumer and competition regulators, including engaging with the Competition and Markets Authority (CMA), the Financial Conduct Authority

(FCA), and the Office of Communications (Ofcom) as members of the DRCF.

- The Insolvency Service, including by referring cases and supporting director disqualification investigations.

Subject to information sharing restrictions in relevant legislation, 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 we regulate (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 memorandums of understanding (MoUs) and publish them on our website.

Where necessary, we work with other regulators and law enforcement to support our regulatory action. For example, we have a robust but fair approach when recovering fines, providing payment plans where debtors are in genuine financial hardship. But if a company seeks to avoid a financial penalty despite being able to pay, we will pursue formal recovery action which can result in insolvency. We have achieved success in obtaining director disqualifications in serious cases to disrupt those who repeatedly break the rules, including by making referrals to the Insolvency Service. Since 2021, we have had direct access to powers under the Proceeds of Crime Act 2002 to conduct our own financial investigations to deprive people of their proceeds of crime.

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. Together with these partners, we formed the DRCF, a non-statutory body. Through the DRCF, we hope to develop this co-operation further. Its goals are to:

- promote greater coherence, so that where regulatory regimes intersect the DRCF helps to resolve potential tensions, offering clarity for people and industry;
- work collaboratively on areas of common interest and jointly address complex problems; and
- work together to build the necessary capabilities, learning from what each regulator is doing and striving to be best in class, both now and in the future.

In support of our fair approach to regulatory action, we share experiences with other regulatory bodies through our membership of the UK Regulators' Network (UKRN). 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 \(DCRF\)](#)

[Regulatory Initiatives Forum](#)

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

To protect the UK public's information rights effectively, we need to co-operate and act internationally. This is reflected in our international strategy that recognises 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 is a key part of our toolbox, allowing us to regulate in a modern, cross-border economy. Indeed, in today's world it is essential to be able to work with regulatory partners across jurisdictions, where information 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 a range of groups, including those set out below. Where appropriate, we co-ordinate our investigative and evidence gathering activity with these partners; either jointly or individually, depending on the circumstances of the case. We may choose to collaborate internationally when other 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 good 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 helped address 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 memorandums 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 forums:

- **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 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 (DGP)**

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 personal 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 aims.

- **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 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 document about how we regulate. It reflects how we focus our efforts and resources to tackle breaches of the legislation we enforce 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 our approach under review and will update it, as and when necessary, to reflect any amendments to the legislation this document 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. We will set out the detailed actions we take each year in our annual plans and will publish our progress against them in our annual reports.

# 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 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 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, taking into account 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 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;
- monitor relevant developments that 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 is 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 require 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);
- serve an assessment notice when carrying out investigations or data protection audits to help us understand how organisations use and store data (under section 146 DPA 2018);
- notify an organisation of alleged breaches of the UK GDPR or DPA 2018;
- enter, inspect and search any premises that an organisation uses, as well as operate and test equipment used for the processing of personal data (under section 154 and schedule 15 DPA 2018);
- 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; or
- 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; and
- approve binding corporate rules (as required by Article 47 UK GDPR).

Under section 197 DPA 2018, we can prosecute a member of the public or an organisation if we believe there is sufficient evidence that a criminal offence has been committed under the DPA 2018 and if we believe that prosecution is in the public interest (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 to 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 (under section 50 FOIA) that 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 what action to take.

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 can prosecute a public authority (or any person who is employed by, is an officer of, or is subject to the direction of the public authority) if there is sufficient evidence that a criminal offence has been committed of altering or destroying records with intent to prevent disclosure and if we believe prosecution is in the public interest (except for offences committed in Scotland, which we would refer to the Procurator Fiscal).

### **Further reading**

[Guide to freedom of information](#)

[FOI and Transparency regulatory manual](#)

## 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 its core role and functions. Regulation 3 lists PSBs covered by the RPSI Regulations.

The RPSI Regulations only apply to accessible information, ie information that is not exempt from disclosure under 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 it holds 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 it applies restrictions on the re-use, the requester should ask for 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 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 under the RPSI Regulations come from the equivalent provisions in FOIA. An ICO investigation could conclude with a decision, recommendation notice or a finding that the RPSI Regulations are 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 INSPIRE Regulations 2009 established a data standards framework designed to make sharing and reuse of spatial data and spatial data services easier. Spatial data is any data with a direct or indirect reference to a specific location or geographical area. The framework requires public authorities to use common standards for spatial data and data services.

The Regulations apply to all public authorities in England and Wales, and Northern Ireland, 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.

### What are our regulatory responsibilities under these regulations?

We have limited responsibilities to consider complaints under the INSPIRE Regulations.

INSPIRE Regulation 9 allows public authorities to restrict public access to data for a number of reasons, for example, the protection of personal data, intellectual property rights or national security.

If a person believes that some or all of the information has been unreasonably withheld, they must first make a complaint directly to the relevant public authority. If the person remains dissatisfied after receiving a reply to the complaint and the reasoning for continuing to withhold the information, they may then complain to us.

### 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, live and automated phone 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, certain provisions of the DPA 1998 relating to our enforcement functions remain in force for the purposes of PECR, even with the introduction of the DPA 2018. These are Part V and sections 55A to 55E (dealing with monetary penalties), Schedule 6 (Appeal proceedings), and Schedule 9 (Powers of entry and inspection) of the DPA 1998.

### **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 National Cyber Security Centre (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 the RDSP's security policies.

Under Regulation 16(2) NIS, if we receive evidence that an RDSP is not meeting its 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 its requirements.

Regulation 17(2) NIS says we can issue an enforcement notice to an RDSP if we believe that it failed to comply with certain duties and requirements (eg a failure to notify an incident under Regulation 12(3) NIS). Regulation 17(2A) NIS further states that, before serving an enforcement notice, 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 under Regulation 17(2) NIS or the duty set out in Regulation 17(3A) NIS, 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 representations may be made about the content of the notice of intention to impose a penalty and any related matters.

Under Regulation 18(3B) NIS 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) NIS, 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) NIS;
- 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 NIS; 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 RDSP to obtain an injunction to enforce the duty or for any other appropriate remedy or relief. However, we may not bring or continue proceedings if an RDSP has appealed under Regulation 19A and the Tribunal has 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) NIS, 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 (eIDAS)

### **What are the eIDAS regulations?**

Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (EU eIDAS Regulation) is an EU 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 the effect, supervision and enforcement of the eIDAS regulations in the UK, which are set out in the Electronic Identification and Trust Services for Electronic Transactions regulations (2016) (the UK eIDAS regulations).

The 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 \(legislation.gov.uk\)](https://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 the IPA?**

Under the IPA, 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 storing this information safely 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 or 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](#)