

# Information Rights Strategic Plan 2017-2021

<b>Contents</b>	<b>Page</b>
Commissioner's message	3
Introduction	6
Our Mission	6
Our Vision	6
Our strategic goals	7
Goal #1: To increase the public's trust and confidence in how data is used and made available	7
Goal #2: Improve standards of information rights practice through clear, inspiring and targeted engagement and influence.	9
Goal #3: Maintain and develop influence within the global information rights regulatory community.	10
Goal #4: Stay relevant, provide excellent public service and keep abreast of evolving technology.	11
Goal #5: Enforce the laws we help shape and oversee.	13
Goal #6: To be an effective and knowledgeable regulator for cyber related privacy issues.	15

## Commissioner's message

We stand today on the edge of a new frontier.

The pace of the digital economy combined with the arrival of a game changing piece of legislation will reshape the data protection landscape.

The General Data Protection Regulation, the centre piece of a package of EU data protection reforms, brings a 21st century approach to data protection legislation. It provides greater protections for the public and enhanced obligations for organisations.

And it brings change for the regulator too. Not only in practical terms, but in the way it reflects what the public expect: more control over their data, greater transparency about how it is being processed.

I've worked as a regulator in this field for many years and my focus has always been on making sure the regulator is relevant. We have a fantastic opportunity to demonstrate our relevance by having a direct impact on public trust.

I believe privacy legislation and an effective regulator can make a difference to how much trust people have in what happens to their personal data. Trust in data flows is fundamental to people engaging in the digital economy.

And trust in both privacy and Freedom of Information regulation is fundamental to democracy. Open government, freedom of information and data innovation are all dependent on a transparent approach to information management.

This strategic plan sets out my mission to increase the trust that the public has in government, public bodies and the private sector: trust in transparency, in the digital economy and in digital public service delivery.

Our strategic approach highlights a commitment to:

- lead the implementation and effective oversight of the GDPR and other live data protection reforms;
- explore innovative and technologically agile ways of protecting privacy;

- strengthen transparency and accountability and promote good information governance; and
- protect the public in a digital world.

My office will do that by encouraging good information rights practices, providing advice and guidance and, where necessary, taking proportionate enforcement action.

We will continue to work proactively with the private, public and third sectors to realise the UK's economic and social potential in the digital economy, and will promote and uphold the UK public's rights to privacy, freedom of information and transparency in government decision making.

We understand that our work will not be without its challenges.

Our main priority is supporting the implementation of the EU data protection reform package in 2018. Preparing business processes and guidance for the GDPR, the Law Enforcement Directive and the ePrivacy Regulation will be the highest priority for us in the first two years of this strategic plan.

The change to the regulatory environment as the UK leaves the EU will also bring challenges. The ICO's future relationship with the European Data Protection Board will be one important dimension.

The pace of change of both legislation and attitudes to personal data brings opportunity, but it brings risk too. To stay relevant in a changing domestic and global political environment, we will need to respond to public concerns and legislative imperatives in relation to privacy, the digital economy, technological advances in the use of data and the digital skills agenda. And we'll need too to retain focus on the other aspects of our regulatory portfolio, notably access to public information.

The ICO is changing to respond to these opportunities and risks. We must grow and maintain the capacity and capability of our workforce as our regulatory responsibilities increase in scope and complexity. We anticipate significant growth in our workforce during the life of this strategic plan, and acknowledge that such growth will come at a time when the skills possessed by ICO staff are in high demand from other organisations.

But we start from a position of strength. Today, the ICO is at the forefront of policy, guidance, direct advice to the public, and enforcement of the UK's data protection and freedom of information laws; shaping how emerging technologies and information practices impact the lives of the UK public. This strategy will make sure we maintain that position in a changing world.

A handwritten signature in black ink, appearing to be 'ED', with a long horizontal flourish extending to the right.

**Elizabeth Denham**  
Information Commissioner

## Introduction

This four year plan sets out the ICO's mission, vision and strategic goals. It is for those organisations, groups and individuals who need to know how we are planning to meet our obligations to the UK public. It is also for those who want to work with us to achieve our goals. This plan covers the period from April 2017 to March 2021.

Our plan supports the statutory responsibilities of the Information Commissioner, Elizabeth Denham, and her office to regulate and promote good practice in line with a range of data protection and freedom of information related legislation.

The Commissioner is also expected to be confirmed as the UK's supervisory authority under the package of EU data protection reforms which apply from May 2018.

Progress against the goals and strategic priorities set out in this plan will be measured and reported annually to Parliament.

The Commissioner allocates specific functions to the directorates and departments which make up the ICO. And drawing down from this overarching strategic plan, each ICO directorate will produce more detailed business plans that describe their priorities and activities.

## Our Mission

To uphold information rights for the UK public in the digital age.

## Our Vision

To increase the confidence that the UK public have in organisations that process personal data and those which are responsible for making public information available.

## Our Strategic Goals

**Goal #1: To increase the public's trust and confidence in how data is used and made available.**

Research shows that public trust in those who process personal and public information is low. As well as being a cause for concern for many and distress for some, this also hampers the growth of the UK and global economy.

The public should have informed confidence in those entrusted with personal and public information. There should be a culture of transparency and accountability amongst those processing personal data or responsible for public information.

We will therefore ensure we understand what contributes to public trust and confidence. In turn we will support organisations to adopt information rights practices specifically intended to increase that trust.

Progress towards this goal will be measured annually through our tracking research.

### **Strategic priorities**

To achieve this culture of improved trust we have identified the following strategic priorities:

- **Increasing transparency**

The public should be able to easily find out and influence how their personal data is being used. And through freedom of information, Parliament decided that public information should be available to the public. The Commissioner has been given the duty to ensure that this happens.

With these principles in mind, we will help the public to understand what to expect from organisations responsible for personal data and public information. We will also make sure those responsible for information have all the support and guidance they need to understand what it means to be transparent and how to embed these practices into their organisation.

In particular, the public should have straightforward access to clear information about data processing. They should expect the highest standards of transparency for processing that has a serious impact on their lives. We should all be able to see, challenge and correct personal records, especially where these contain detail of particular sensitivity.

We will also work in particular to promote transparency of digital processing - including the use of big data, artificial intelligence and machine learning - where opaque or invisible practices can pose a particular risk to public trust and confidence.

- **Creating a culture of accountability**

Organisations should provide assurance to the public, and where necessary to us as the regulator, about how they manage data protection and privacy.

Promoting accountability will be a priority activity for the ICO – in guidance, toolkits and other communications with stakeholders.

We will define the parameters of good information rights practice and clearly explain what good practice looks like to both users of data and the public. We will develop a privacy management framework that supports the implementation of accountability programmes.

We will champion a culture of both innovation and accountability. Privacy protections should be built into innovation, by design and by default.

We will develop frameworks to enable the ICO to accredit codes of conduct and certification schemes as mechanisms to enable organisations to demonstrate the effectiveness of their accountability measures.

We will provide organisations with support and tools to develop accountability frameworks which help them deliver their responsibilities under evolving data protection regulation and give the public confidence in their approach.

We will strive to ensure that the public have the opportunity to understand their information rights and how to hold organisations to account.

Our assurance functions will be used to educate and engage as much as



to audit and critique. We will actively seek exemplar organisations to help illustrate good practice which protects people's personal information.

## Goal #2: Improve standards of information rights practice through clear, inspiring and targeted engagement and influence.

We want to encourage and inspire those we regulate to achieve the highest possible standards in their information rights practice.

We also want to be a trusted adviser to law makers and those who influence them to ensure the UK information rights regulatory landscape is clear and supports those committed to compliance and higher standards of good practice.

We will have achieved this goal when the public and those we regulate see us as the authoritative arbiter of information rights, delivering high quality, relevant outcomes.

We will measure our progress towards this goal through independent stakeholder research.

### **Strategic priorities**

In working towards this goal we will focus on the following strategic priorities:

- **Leadership**

We will scan the horizon for new technologies and new risks to information rights, challenge stakeholders and pull back the curtain on practices the public should know about. We will be a critical friend to government and organisations alike, doing whatever we can to place information rights issues and best practice high up their list of priorities. We will seek to embed into new technologies privacy by design and default.

- **Excellent guidance**

We will produce reliable, helpful and timely guidance, particularly as the regulatory framework under which we operate changes.

- **Assurance**

Advice, guidance and assurance, used effectively, will reduce our need to enforce and enable us to focus on high public impact cases. We will publish good practice guidelines and enable organisations to come to us and explain how they comply.

- **Advising and influencing Government**

With such widespread and significant regulatory and legislative change in data protection expected throughout the life of this strategic plan, we will give particular focus to our engagement, including in Scotland, Wales and Northern Ireland, with policy makers, legislators and other groups who represent the public. We will make the case for an effective, modern information rights regime that promotes public trust and understanding.

- **Partnership working**

Throughout all parts of the UK we will further develop work in partnership with key public, private and third sector stakeholders.

We will work with other regulators, public bodies and representative associations of organisations to enhance our knowledge and achieve our aims. We will do this through co-operation agreements and direct engagement.

With regard to the EU data protection reform package we will work to prepare stakeholders in all sectors up to, through and after the transition to the new regulatory regime. We will also ensure the public have the opportunity to understand their rights and how to exercise them.

### **Goal #3: Maintain and develop influence within the global information rights regulatory community.**

Information rights regulation, and in particular data protection regulation, has an increasingly international dimension. Effective protection of the UK public's personal information becomes increasingly complex and less visible as data flow across borders so the UK needs a regulator with global reach and influence.

As the UK prepares to leave the European Union, the formal relationship between the ICO and EU data protection authorities will change. While our

relationship with our EU partners will remain highly important and a strong focus in the transition period, there will also be opportunities for new or enhanced relationships with information rights regulators and communities on the worldwide stage.

We will measure our progress towards this goal through third party feedback about our international work and the measures of success set out in our international strategy.

### **Strategic priorities**

To expand and enhance our international work we will have the following strategic priorities:

- **Develop an International Strategy**

We will put into action an International Strategy designed to achieve global reach and influence for the ICO.

- **Creating and maintaining effective relationships**

We will continue to play a full part in EU data protection working groups and boards until the UK leaves the EU and work closely with EU partners and institutions post-Brexit, including the European Data Protection Board and other relevant EU data protection functions.

We will work closely with Government to define our role in any transitional arrangements and in the legal environment following the UK's departure from the EU.

As the global regulatory environment changes and the UK leaves the EU, we will seize opportunities to engage with information rights regulatory regimes and communities outside the EU, with the aim of establishing effective networks and relationships in the UK public interest.

### **Goal #4: Stay relevant, provide excellent public service and keep abreast of evolving technology.**

Innovations and advancements in technology, and the parallel rapid growth and availability of data, have the potential to enhance and ease the lives of people and organisations throughout society and the economy. This potential is heightened by the continued growth and availability of data, including data from new sources such as the Internet of Things.

Far from limiting or preventing these developments, we want to ensure that privacy enhancing techniques and tools are built in by design, enabling data protection good practice to become an essential aid to effective innovation.

The use of big data, artificial intelligence and machine learning has significant implications for privacy and data protection. We want to ensure that privacy and data protection considerations are integral to big data analytics.

Maintaining and increasing our technical understanding of the environment we regulate goes hand in hand with our own use of technology in our services and working practices as we continue to invest in technology and skills the public would expect of a modern regulator.

We will measure our progress towards this goal through the measures set out in our respective Technology and Resource and Infrastructure strategies.

### **Strategic priorities**

To maintain our relevance in an ever more technologically sophisticated world, we will have the following strategic priorities:

- **Working with innovators**

We will develop the capacity to assist organisations by ensuring our technological proficiency. We will create a safe space for innovation, by developing a regulatory Sandbox where new technologies can be investigated and tested at an early stage of technological innovations to prevent later regulatory concerns.

- **Develop a Technology Strategy**

A new Technology Strategy will outline our means of adapting to technological change as it impacts information rights and enable us to plan ahead for the arrival of new technologies.

- **Develop a Resource and Infrastructure Strategy**

A new Resource and Infrastructure strategy will ensure we have the capacity and capability to succeed as our regulatory role develops.

- **Research and understanding**

We will keep up with the pace of change in the adoption of new technology, exploring the implications of innovation for privacy rights and supporting ground-breaking research. Where appropriate we will commission specific research or issue calls for evidence. We will build on the success of our grants programme, and continue to support independent academic and public interest research into applied information rights products and solutions.

### Goal #5: Enforce the laws we help shape and oversee.

Whilst our initial approach will be to encourage and inspire good practice and compliance, we will not shy away from taking formal regulatory action where unlawful practices need to be halted, rectified or exposed.

We understand that the proportionate and effective use of our regulatory sanctions serves as an important deterrent to those who risk non-compliance with the law.

Under the EU General Data Protection Regulation (GDPR) we will also see an increase in the scale and impact of the sanctions at our disposal. We are committed to using these increased powers in ways which target the most serious areas of non-compliance.

We will measure our progress towards this goal through a combination of independent stakeholder and annual track research.

### **Strategic priorities**

To maintain our effective and proportionate regulatory response we will have the following strategic priorities:

- **Develop a new Regulatory Action Policy**

A new Regulatory Action Policy will be implemented as part of our preparations for the forthcoming EU data protection reform package. It will be laid before Parliament in 2018.

- **We will take fair, proportionate and timely regulatory action**

We will use the information gathered from the public, those we regulate and other stakeholders to identify areas of poor practice or non-compliance. We will take regulatory action, where appropriate, in those areas which most directly and effectively further our strategic vision.

We will use all of the powers and tools available to us to improve practice, but be proportionate and fair in doing so.

- **We will further improve our work to tackle the public challenge of nuisance calls**

We will continue to ensure that lead generation and data broking organisations are compliant with the law and we will continue to provide tools to the public to enable them to report nuisance calls to us easily and quickly.

- **We will prioritise issues and cases of significant potential public impact**

We will develop an Intelligence Strategy to enable us to see and take action on issues as they emerge and deal with those of significant potential impact as a high priority.

### Goal#6: We will be an effective and knowledgeable regulator for cyber related data protection matters.

We will have an expanded role involving a range of cyber related data protection and network information issues; we want to provide a world class reporting, assessment and investigation service to ensure UK citizens are protected from harm.

The implementation of the GDPR, eIDAS and the NIS Directive will bring enhanced reporting requirements, with more exacting timescales, for data and network security breaches requiring a cyber incident response. The new legal framework will bring more stringent requirements to safeguard personal data and systems by default and design, as well as new powers for the ICO around both proactive assessment of systems and networks and the investigation of cybersecurity breaches.

We want to be able to respond to GDPR, eIDAS and NIS breaches effectively, co-ordinating with the UK national response process ensuring

that we have the necessary powers, information sharing agreements and capacity and capability in place to do so.

We will deploy suitably qualified and accredited staff to assess and investigate information systems, breach reports and proposals from business and other organisations. We will also gather and secure evidence, including gaining appropriate digital forensic understanding of a breach, effectively as part of our investigative processes.

We will communicate our role and advice appropriately and in a clear manner during the initial response phase of an incident. We will be effective in signposting the public to helpful sources of advice and support about how they can protect themselves from any impact of the breach. We will ensure that those we regulate play a full part in protecting the public from any harm arising from incidents.

Where risks to UK Citizens cannot be easily mitigated but innovation is important we want to offer opportunities for organisations to test products and services in a safe manner through close supervision in a regulatory sandbox.

We will measure our progress towards this goal through stakeholder feedback and reporting our performance against our published service standards.

### **Strategic priorities**

To achieve this goal we will prioritise the following actions:

- We will provide an effective service meeting an expanded range of customer's and stakeholder's breach reporting and incident response needs. We will prioritise our response to significant data breaches affecting large numbers of UK citizens.
- We will strengthen our relationships with other relevant agencies working in this area. This will include a programme of secondments and apprenticeships to build our in house capability and capacity.
- We will agree a core suite of information for the public, agreed with other stakeholders involved in the UK incident response mechanism, as the basis of communications to describe our and our partners' respective roles during live incidents.

- We will participate in national incident response drills, to train staff and test the effectiveness and readiness of arrangements. We will debrief incident responses and investigations to gather learning and improve our services in future.