Information Commissioner's Office

Technology Strategy 2018-2021

ico.
Information Commissioner's Office

Contents

Commissioner’s message 3
Introduction 4
Our technology goals 4
Annex A: Our technology priority areas 2018-2019 8

Commissioner's message

Technology is driving changes to the societal, political, legal and business environment that the Information Commissioner's Office (ICO) needs to regulate. The most significant data protection risks to individuals are now driven by the use of new technologies. The risks are broad – from cyber-attacks to the growth of artificial intelligence and machine learning.

The Digital Economy is the fastest growing area of the UK economy. New technologies can provide significant societal and economic benefits across the private, public and third sectors. Whole new fields are emerging, such as EdTech, FinTech and HealthTech. The UK Government has placed digital at the heart of its new Industrial Strategy.

My Information Rights Strategic Plan for 2017-2021 makes clear that staying relevant in the context of ever changing technology must become a core component of the ICO's strategic goals, otherwise the ICO will fail to deliver the regulatory outcomes the public expect.

Changes in technology were one of the key drivers in reforming European data protection law, leading to the introduction of the General Data Protection Regulation (GDPR) in May 2018. The GDPR contains new provisions to better regulate the risks arising from technology, including data protection by design and data protection impact assessments.

These advances need not come at the expense of data protection and privacy rights – the ICO's approach to technology will be underpinned by the concept that privacy and innovation are not mutually exclusive. When they both work together this creates true trust and data confidence. Technology is therefore viewed by the ICO as a risk and an opportunity.

It is for these reasons that I have decided to publish the ICO's first Technology Strategy.

Elizabeth Denham
Information Commissioner

Introduction

This Technology Strategy supports our Information Rights Strategic Plan 2017-2021 and in particular Goal #4: 'Stay relevant, provide excellent public service and keep abreast of evolving technology' and the specific strategic priority to 'Develop a Technology Strategy' that 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'.

The Technology Strategy seeks to develop and enhance technical knowledge and understanding at the ICO and to ensure we effectively communicate these to both organisations and individuals. Knowledge of how technology effects information rights is not a niche area for the ICO or just the responsibility of one ICO department. This work will be spearheaded by our new Technology Policy Department, but we will seek to embed awareness of technology across the ICO's teams.

The Technology Strategy explains our eight technology goals and how we intend to achieve them. From our assessment of the risks and opportunities arising from technology, looking at current, near and distant perspectives we have also identified three priority areas that we will focus on in 2018-2019.

We will prioritise work which contributes to the ICO's knowledge and understanding in these key areas. We will review and update the Strategy annually to reflect the rapid pace of change within the technological environment and the increasing importance of technology to the processing and protection of personal data. This will ensure that the ICO is fit to respond to new challenges, proactively identify issues, and take opportunities as they arise.

This Strategy does not cover the ICO's own use of digital and IT services to support its operational activity – the detail of this is set out in the ICO Resource and Infrastructure Strategic Plan.

Our technology goals

Technology goal #1: To ensure effective education and awareness for ICO staff on technology issues.

- We will develop training programmes for ICO staff to develop their technical knowledge and understanding at a level appropriate to their role. This training will aim to develop core knowledge of how essential technologies work and further learning on new and emerging technologies. This will also include technology briefings for the ICO Senior

Leadership Team and Department Heads. We will seek accreditation for technology skills where appropriate.

- We will develop competencies for staff in roles connected to technology and add these to job descriptions.
- We will develop internal knowledge resources and briefings to ensure that ICO staff can refer to key information about technology.
- We will further develop our internal technology advice service that will ensure ICO staff can access in-depth or specialist technical knowledge and understanding when required.

Technology goal #2: To provide effective guidance to organisations about how to address data protection risks arising from technology.

- As well as developing guidance to support the technology priority areas we have identified, we will update our existing technology guidance to reflect the requirements of the new provisions in the GDPR, the Directive on security of Networks and Information Systems (NIS) and ePrivacy Regulation.
- We will promote the use of data protection design by default, and demonstrate how these contribute to UK economy and growth. We will also write new guidance about these provisions in the GDPR. Guidance and compliance advice provided by the ICO will be technically feasible and proportionate.
- Following on from our successful report on the data protection implications of Artificial Intelligence (AI) and machine learning will produce further reports on emerging technology issues.
- We will publish a report on 'lessons learned' from cyber breaches reported to the ICO and technology issues emerging from Data Protection Impact Assessments annually.
- We will keep organisations informed about emerging risks and opportunities arising from technology in an appropriate and timely manner. This will include blogs, social media and webinars.

Technology goal #3: To ensure the public receive effective information about data protection risks arising from technology.

- We will write new content for the ICO website to ensure that we keep individuals informed about emerging risks and opportunities arising from technology in an appropriate and timely manner.

- We will develop new partnerships to broaden our messages to the public about data protection risks and opportunities arising from technology. We will seek to amplify messages and key information from trusted partners such as National Cyber Security Centre (NCSC).
- We will ensure that the outputs from our GDPR consumer messages project can be tailored and used to provide information about how GDPR rights interact with mainstream and new technologies.

Technology goal #4: To support and facilitate new research into data protection risks and data protection by design solutions.

- We will draw on high quality internal and independent external research and expertise that is relevant to our technology priority areas to develop a comprehensive understanding of these technologies. We will continue to build relationships with research and development stakeholders to inform and educate ICO policies.
- We will use the ICO's Grants Programme to support research and data protection by design solutions.
- We will use business intelligence, including annual track surveys, to understand new areas of public concern and address frequently asked queries.
- We will carry out research and investigations into new and emerging technologies in order to inform our future priority areas.

Technology goal #5: To recruit and retain staff with technology expertise to support delivery of the strategy.

- In line with the ICO's strategic approach, we will use secondees from external organisations to complement and support our established technology team.
- We will also explore the possibility of establishing technology apprenticeships at the ICO, working with relevant universities and other education partners.
- We will establish a panel of forensic investigators to support our regulatory work.

Technology goal #6: To establish new partnerships to support knowledge exchange with external experts.

- We will develop a new stakeholder engagement map focused on technology. The ICO will seek to engage with the following communities to develop stronger or new partnerships:

  - Professional bodies focused on technology
  - Academic technology networks and University departments focussed on technology
  - Public sector technology networks
  - Industry bodies focused on technology

- We will work with cross-sector bodies to embed data protection by design in emerging standards.
- We will establish Technology Fellowships for post-doctoral experts to enable us to increase our in-house advice and expertise on technology priority areas. Our first appointment will be a two-year post-doctoral role to investigate and research the impact of artificial intelligence on data privacy, encompassing big data and machine learning.
- We will revise and reconstitute our technology reference panel with new terms of reference to ensure we receive expert advice and strategic insight into emerging technologies.
- We will develop a new 'call for evidence' process to enable us to receive insight into the data protection risks and opportunities posed by different technologies, linked to the priority areas listed above. We will also hold expert roundtables on each of the priority areas.
- We will establish a new annual ICO conference on Data Protection and Technology to showcase the latest research on data protection risks and data protection by design solutions, including outcomes from the ICO's grants programme.

Technology goal #7: To engage with other regulators, international networks and standards bodies on technology issues related to data protection.

- The ICO's International Strategy sets out the goals for international activity. It makes clear that the ICO will prioritise international engagement on issues related to global privacy risks arising from the application of new technologies. We will also explore new links with international bodies and regulatory networks that do not focus on data protection but have an important influence on developing global technology standards that affect data protection.
- We will continue to engage with the Article 29 Working Party Technology sub group and International Working Group on Data Protection in Telecommunications 'the Berlin Group'.

Technology goal #8: To engage with organisations in a safe and controlled environment to understand and explore innovative technology.

- We will establish a 'regulatory sandbox', drawing on the successful sandbox process that the Financial Conduct Authority has developed. The ICO sandbox will enable organisations to develop innovative digital products and services, whilst engaging with the regulator, ensuring that appropriate protections and safeguards are in place. As part of the sandbox process the ICO would provide advice on mitigating risks and data protection by design.
- In 2018 we will consult and engage with organisations about implementation of a sandbox.

Annex A: Our technology priority areas 2018-2019

The delivery of the goals above is underpinned by a process of regularly identifying technology priority areas, to ensure we put the focus and resources where there are the greatest risks.

We have identified the following priority areas for 2018-2019.

We will develop an action plan for each priority area which we will review and update annually. The list will also be reviewed annually.

Priority area #1: Cyber security

Risks to cyber security are key threats to the personal data collected, stored and transmitted by a range of organisations and should remain a priority area for the ICO in terms of enforcement and policy. There will continue to be threats to infrastructure, networks, systems, Internet of Things devices, smartphones and tablet devices in addition to other industries as these continue to introduce "smart" features (such as connected vehicles). The ICO's strategic approach to cyber security is set in the Information Rights Strategic Plan.

Priority area #2: Artificial intelligence, big data and machine learning

Artificial intelligence, big data and machine learning are now a key component of the Government's industrial strategy, seeking to place the UK at the front of emerging digital technologies.

These technologies can utilise high volumes of personal data from a wide ranges of sources – making decisions and providing new insights about individuals. The technologies are driven by cloud computing platforms which enable the storage and processing power to be used at scale. Data protection and privacy law will be a core component in any broader ethical framework for decision making about AI. Deployment is taking place in the public and private sectors. Examples include new facial recognition tools in the law enforcement sector and use of social scoring in credit and finance sectors. The ability for AI to intrude into private life and effect human behaviour by manipulating personal data make highlighting the importance of this topic a priority for the ICO.

Priority area #3: Web and cross device tracking

The use of HTTP cookies has not diminished although a range of alternative methods of performing tracking online have emerged and become more common. For example device fingerprinting, browser fingerprinting and canvas fingerprinting. This is likely to continue as more devices connect to the internet (IoT, vehicles etc.) and as individuals use more devices for their online activities. These new online tracking capabilities are becoming more common and pose much greater risks in terms of systematic monitoring and tracking of individuals, including online behavioural advertising. The intrusive nature of the technologies in combination drives the case for this to be a priority area.