Information Commissioner's Office Innovation Plan

April 2017

ico.
Information Commissioner's Office

Introduction

The Information Commissioner’s Office (ICO) is the UK’s independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Information Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

The legislative and enforcement frameworks that the ICO works within are primarily:

- The 1995 Data Protection (DP) Directive (transposed into UK law through the Data Protection Act 1998) which gives citizens important rights, including qualified rights to know what information is held about them and to have removed or corrected information that is wrong. Organisations that process personal data are obliged to manage the information they hold about individuals in accordance with eight data protection principles.
- The Freedom of Information Act 2000 (FOIA), which gives people a general right of access to information held by public authorities and requires public authorities to proactively publish information.
- The Privacy and Electronic Communications Regulations 2003 (PECR) which supports the Data Protection Act by regulating the use of electronic communications for unsolicited marketing to individuals and organisations.
- The Environmental Information Regulations 2004 (EIR) which give people the right to request environmental information from public authorities and requires public authorities to make environmental information available proactively.
- The Information Commissioner has a limited supervisory role under the Investigatory Powers Act 2016.
- The Information Commissioner also has a role under the Re-use of Public Sector Information (RPSI) Regulations 2015 and eIDAS, EU Regulation No 910/2014 on electronic identification and trust services.

We are pleased to provide this innovation Plan as part of assurance that the UK regulatory framework is working effectively to support innovation and disruptive business models and that, as a regulator, we are using innovation to deliver our own work more effectively and to reduce burdens on business. We have considered three areas:

- How legislation and enforcement frameworks could adapt to new technologies and disruptive business models to encourage growth.
- An assessment of how new technology is likely to shape the sectors being regulated.
- Actions for how regulators could better utilise new technologies to generate efficiency savings and reduce burdens on business.

This plan will cover each of these areas in detail.

How legislation and enforcement frameworks could adapt to new technologies and disruptive business models to encourage growth

We use a number of methods to ensure that we are aware of, up to date with, and respond to new technologies and disruptive business models.

Working with external stakeholders

We established a Technology Reference Panel in December 2011 that meets at least twice a year and provides impartial expert advice on technological issues affecting information rights, covering, as far as possible, the following areas:

- Records management
- Computer science
- Biometrics
- Surveillance technologies such as CCTV
- Mobile and fixed-line telecommunications
- Delivery of on line services
- Database development
- Data matching, mashing and mining
- Information sharing
- Identity management
- Information security
- Information assurance
- Privacy enhancing technologies

This is an example of 'open policy development', using experts from professional, representative and advisory bodies to provide independent views on general developments and trends or particular issues in the field of technology and how we might adapt and respond to them.

In addition, we engage directly with businesses at the forefront of technological change, including global tech companies as well as small companies trying new business models. We provide a full suite of guidance on our website, a telephone helpline, written enquiries services and individual liaison named contacts for strategic stakeholders. One of the aims of our liaison and advice work is to inform organisations about privacy considerations and to find ways of achieving business objectives, promoting innovation alongside compliance with data protection law. Organisations are encouraged to use these services to discuss business plans in a 'safe space' and to work closely with us as projects and products are developed. In March 2017 we blogged about Big data and the insurance sector outlining our work with the Financial Conduct Authority to deliver a forum to discuss the use of data in retail general insurance. A summary of the forum discussion is available via the blog post.

We recently contributed to an industry led event, the Design Jam- Trust, Transparency and Control, which aimed to raise the profile of privacy and data protection amongst designers and embed users and their rights into app development. We will continue our engagement in this regard and will feed the knowledge gained into our work on transparency guidance at a European level.

We work closely with other regulators and government departments in the field, for example Department for Business Innovation and Skills, on the digital economy and nuisance calls and texts, and Communications-Electronic Security Group (CESG) within GCHQ.

We are active members of international forums on technology issues related to information rights such as:

- Working Party 29 Technology Subgroup (as Chair);
- International Working Group on Data Protection in Telecommunications; and
- The Internet Privacy Engineering Network.

Guidance

The current data protection legislative framework is principle based. The interpretation of the principles in relation to technology is done through our guidance, on which businesses are routinely consulted. We published our revised code of practice Privacy notices, transparency and control on 7 October 2016. It emphasises the importance of transparency in building consumer trust which is key to further growth of the digital economy. It advises businesses to use technology and to be innovative about how they inform consumers about how they use their information. Further examples of guidance with a technology focus include:

- Mobile apps
- Social media and the Data Protection Act
- Cloud computing
- ID scanning in pubs and clubs
- Encryption
- Wi-Fi location analytics
- A practical guide to IT security

We provide businesses with guidance and advice on how to integrate data protection as they develop business ideas, products and services using a ‘privacy by design’ approach including tools such as the Privacy Impact Assessment code of practice. Our aforementioned big data paper also includes specific advice about conducting Privacy Impact Assessments in a big data context, having consulted with business applying this technique.

General Data Protection Regulation (GDPR)

The legislative framework for data protection is due to change considerably in the next two years as the government has now confirmed a commitment to implement the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LE directive) as well as the e-Privacy Regulation which is still in development. Organisations will have to comply with the GDPR from 25 May 2018.

The GDPR comments on the need to ensure the data protection framework adapts to new technology:

> Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collection has increased spectacularly. Technology allows both

> private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.
>
> These developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Individuals should have control of their own personal data and legal and practical certainty for individuals, economic operators and public authorities should be reinforced.

The GDPR includes a requirement, in certain circumstances, for organisations to tell affected individuals where there has been a personal data breach, a new right to portability of data to allow transfer between providers, additional obligations in respect of children’s data, the right to access to personal information, the right to object to processing in specified circumstances, and restrictions on the use of data for profiling and automated decision making (discussed in more detail later) amongst other issues.

The e-Privacy Regulation (e-PR) is still being developed and the plan is that it will come into effect alongside the GDPR in May 2018. Under current proposals the e-PR would apply to organisations anywhere in the world if they provide services to people in the EU, to services offering ‘over-the-top communication channels and to businesses providing customer Wi-Fi access. It would mirror the GDPR two-tier fines, shift focus from website cookie banners to users’ browsers settings and tighten marketing rules.

The impact of changes to the information rights legislation on organisations, members of the public and how technology is used will be reviewed in detail as we update our guidance to reflect the reforms. We have a dedicated data protection reform section on the ICO website which provides all the latest information about our work in this area including the most recent guidance we have produced to assist organisations with their preparation.

An assessment of how new technology is likely to shape the sectors being regulated

We have considered three areas of new technology that relate to personal data in more detail:

- the internet of things;
- Artificial Intelligence (AI), automated or rule based decision making and big data; and
- remotely piloted aircraft systems (RPAS) or drones.

We have taken the following analysis from the ICO paper 'Threats and Opportunities to Information Rights Arising from Technology'. This is an internal paper, made available to ICO staff and Management Board and kept under review, written by Dr Simon Rice the head of our newly formed Technology Policy Department. It focuses on horizon scanning for new developments in technology.

The internet of things

The vision of a connected home has long been promised, however, as more and more consumer devices are being shipped with connection capabilities built into them (e.g. Wi-Fi, Ethernet, sensors etc.) this is brought ever closer to reality. So far, the internet of things has been most closely associated with machine-to-machine communication in manufacturing and power, oil and gas utilities. However, it is a growing paradigm that continues to influence our lives.

With the rollout of smart metering throughout the UK, access to live data will become more familiar to UK households. Connecting sensory devices such as lighting to games consoles may also provide an enhanced experience for users, driving widespread adoption. Furthermore, internet connectivity is becoming an increasingly common feature of new consumer goods such as televisions and mobile devices. It is inevitable that homes will be more connected to external providers offering their convenient services.

The UK has an aging population, placing an ever increasing demand on health and social care services. It is perhaps inevitable that innovations such as tele-care and other assisted living technologies are introduced to ease the burden on the current healthcare system.

As with many developments that relate to personal data, the data available from a connected network could be stored and processed by a third party to gain insight into the routine, preferences and habits of the individual or family. This could be beneficial in recommending more appropriate energy tariffs or for monitoring safety. However, this also opens the door to potential surveillance, tracking and profiling for a variety of means. The data are also a target for attack by a malicious third party, again for a variety of means.

Early examples of the internet of things within this environment include; Proteus Digital Health, who have developed an ingestible sensor, which tracks whether a patient is taking their medication on schedule. A Swiss company called Vigilant, has developed a smart insulin injection tracker to help diabetic patients manage their health. The Tracker, Bee+ is an electronic cap that fits most insulin pens and then transmits the insulin data to a smartphone app. Finally, Pixie Scientific have developed smart diapers that analyse a patient's urine to check hydration levels and identify signs of infections. Data is sent to a smartphone app.

The ICO is committed to helping organisations use these new technologies where they benefit users in the ways outlined above whilst ensuring any risks are mitigated. Mitigations to any possible threat to personal data could include appropriate default security measures, for example, by the home router to block external access which would mitigate the risk of external attack. Furthermore the default position of not sharing data with the device provider and requiring suitably informed consent would further reduce the risk of misuse of personal data. Other mitigations include application of security patches for all internet of things devices, changing default passwords and even blocking connections on specific ports (23 or 80) from the outside world.

Finally, we published a blog on the Internet of Things in July 2016.

Artificial Intelligence (AI), automated or rule based decision making and big data

Big data refers to datasets which are so large, flow fast and often contain different forms of data that were difficult to process using traditional techniques. New methodologies have now been developed to store, analyse and visualise these huge volumes of data. With increased computing strength and complexity, data miners or data scientists are able to gain a more comprehensive understanding of data. As a result, greater volumes of data can be collected with a view to being processed in addition to processing existing datasets which may not have been analysed or combined previously.

As computing power increases and new algorithms are developed the ability of computers to generate creative works will also increase. This may include, for example, pooling live and historical information from the internet to produce an assessment report to highlight key points and messages. Using this intelligence, computers could be implemented in many key decision making roles. Big data is becoming widespread in the public and private sector.

The ICO recognises that the introduction of automated decision making will bring a huge range of benefits for individuals including faster application processing times, but it is unlikely that a system will ever be 100% accurate and an appropriate fall back process must be in place to deal with these errors. Even with a small margin of error, if the number of decisions is sufficiently large, this will still impact on a significant number of individuals.

Organisations collecting and publishing volumes of data and those undertaking big data analysis must be reminded of their obligations under the Data Protection Act. There should also be an appropriate level of communication with the individual concerned to ensure that they are aware that automated processing has taken place and they are aware of their right to have this decision reviewed.

As mentioned earlier we published our paper on Big data, artificial intelligence and machine learning in March 2017 and we will continue our work in these fields as one of our information rights policy priorities. For further information, please also see the International Working Group on Data Protection in Telecommunications working document.

We have recently established a new International Strategy and Intelligence department to deliver our international strategy. The dedicated research and intelligence team is building on existing networks to share experience and knowledge about global information rights issues arising as a result of techniques such as big data analytics.

The General Data Protection Regulation, as referred to above, contains reference to automated decision making based on personal data. In particular:

> The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing, which produces legal effects concerning him or her or similarly significantly affects him or her, like automatic refusal of an on-line credit application or e-recruiting practices without any human intervention. Such processing includes also 'profiling' consisting in any form of automated processing of personal data evaluating personal aspects relating to a natural person, in particular to analyse or predict aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements as long as it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision making based on such processing, including profiling, should be allowed when expressly authorised by Union or Member State law, to which the controller is subject, including for fraud and tax evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of EU institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child, to express his or her point of view, to get an explanation of the decision reached after such assessment and the right to contest the decision.
>
> In order to ensure fair and transparent processing in respect of the data subject, having regard to the specific circumstances and context in which the personal data are processed, the controller should use adequate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure in particular that factors which result in data inaccuracies are corrected and the risk of errors is minimized, secure personal data in a way which takes account of the potential risks involved for the interests and rights of the data subject and which prevents inter alia discriminatory effects against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, genetic or health status, sexual orientation or that result in measures having such effect. Automated decision making and profiling based on special categories of personal

data should only be allowed under specific conditions.

We are leading work at European level on guidance for organisations on the GDPR provisions on profiling. To inform our work we ran a workshop on profiling at our Data Protection Practitioners Conference on 6 March 2017 and we will moderate a similar session at a European stakeholder engagement event in April. A short public consultation on the subject is also imminent so that we obtain views from a range of businesses and organisations with an interest.

Remotely piloted aircraft systems

Remotely piloted aircraft systems are a subset of unmanned aerial vehicles and are colloquially known as drones. Drones are typically small lightweight aircraft which fly without an individual on-board. Flight is controlled either autonomously or remote control by a (not necessarily) ground-based pilot.

Drones have a wide range of potential uses depending on the sensors and communication capabilities they are equipped with. The largest military vehicles can carry surveillance equipment and weapons. Small vehicles for personal or hobbyist use may be equipped with a camera and battery permitting 20-30 minutes flying time.

Additional commercial uses include surveillance, search and rescue, logistics, scientific research and patrol. It has also been reported that vehicles could be equipped to deliver internet services.

The greatest impact is likely to come from vehicles equipped with video capabilities and the recording of individuals, in a number of cases without their knowledge. Additional sensors may also collect personal data.

If internet services were delivered by aerial vehicles, there is potential for all communications to be monitored by the provider of the communications service.

A number of UK-based organisations have run trials with the technology including law enforcement. Consumer devices are available from £200-£300 for a device with a camera-equipped device which streams images live to a smart phone. The European Commission has also recently launched a policy framework and roadmap to promote the sector.

On 22 August 2016 the European Aviation Safety Agency (EASA) issued a first draft of a Prototype Commission Regulation on Unmanned Aircraft Operations. The ICO is developing its policy in this area and we are responding to the EU consultation with data protection authorities on the prototype regulation.

The ICO also recently responded to the UK government consultation, Unlocking the UK's High Tech Economy Consultation on the Safe Use of Drones.

A high level of transparency will be required to give individuals sufficient information regarding the data being processed. This is going to be particularly challenging if the vehicle is air-borne. Organisations' use of RPAS will benefit from conducting a privacy impact assessment to address the risks such as the loss or theft of the device.

For further information, see the ICO's revised CCTV code of practice and the International Working Group on Data Protection in Telecommunications Working Paper on Privacy and Aerial Surveillance.

Actions for how regulators could better utilise new technologies to generate efficiency savings and reduce burdens on business

We are committed to using technology to develop our services. The focus of our work in providing digital services has been to avoid unnecessary transactions for organisations with a regulator, and make sure that when transactions are needed they are as clean and efficient as possible.

We have improved our website to make it easier for the public to raise concerns with us and also improved the ease with which those we regulate can access advice and guidance. We are also considering the feasibility of developing tools such as a privacy notice generator which would likely help small to medium sized organisations in particular to meet their transparency obligations.

We are also establishing an ICO Grants Programme which will make financial support available to not-for-profit organisations for applied research into innovative solutions to privacy challenges posed by new technologies such as artificial intelligence and machine learning. We will share details of the results to assist organisations and raise their awareness of technological solutions to privacy related issues available to them.

We have also introduced new technology to make it easier for the public and organisations to contact us.

Digital services

We are developing a range of new digital services:

- a new tool to report nuisance calls and marketing messages to us such as spam texts and cold calls which was shortlisted for a national award in digital service excellence;
- an online complaint checker that allows members of the public to see what might happen if they raise a concern with us;
- our notification fee collection has also moved online, away from cheque payments, providing a platform for efficient registration and fee collection. This has also been used to improve one off payments, such as conference fees;
- an online data protection self-assessment toolkit, aimed at small and medium sized organisations which allows them to assess their compliance with data protection legislation, gives links to ICO and other organisations’ guidance and gives recommendations and suggested actions. We are planning to update this toolkit to reflect the requirements of the GDPR. This has proved very popular and generated extremely positive feedback from stakeholders;
- ICO hosted webinars offering practical information and guidance about a range of information rights topics and issues. Recent webinars with hundreds of registered attendees have included, Cybersecurity, Data Protection for SMEs, Data Protection for Law Firms and Direct Marketing;
- our ‘Live Chat’ service on our website has succeeded in reducing the total number of front line transactions needed to meet the needs of our customers. Customers, and in particular organisations, who would previously call our Helpline or send us a letter or email are now using our live chat service. They receive answers to their questions much more quickly and the service is also more efficient, and less expensive, to support. We plan to develop the use of this new service in the coming months;

- a stakeholder management tool which allows us to be more efficient and link up information provided by business so they can 'only tell us once' **Proactive disclosure**

We have introduced a new service which sees us proactively disclose raw data relating to all complaints, concerns and self- reported incidents we deal with. This is in line with our commitment to 'Open Data' and allows the organisations we regulate to see at a glance the number of cases their information rights practice is generating for the regulator.

We have been proactive in sharing our own internal guidance to allow organisations to better understand the decision making processes at the ICO. An example is the publication of our internal 'lines to take' database for Freedom of Information work. However, it is important to clarify that we have subsequently amended our approach to guidance to include as much detail as possible in our external facing guidance so that organisations have access to as much information as possible to help them meet their information rights obligations.

We will also continue to make our decisions as accessible as possible, as they are a relevant resource for people looking to raise concerns with us.

Future progress

Looking forward, we will continue to develop our digital delivery and it is likely that changes to data protection legislation will require us to implement a number of new or expanded services which we will look to deliver using new technology where feasible. The potential volume of work resulting from these regulatory changes will necessitate the development of technologies to support this transactional work. We are working with businesses and the public sector to prioritise this work and to develop a timetable of how the changes will be implemented. This is a complex area of work and we are committed to developing, and sharing, a full timetable for implementation with stakeholders and ensuring that innovative solutions are adopted to maximise benefits for us and those we regulate.

We are looking at options to develop technologies to support online booking systems, so members of the public can make an appointment to see ICO staff online in a single transaction. We are also interested in developing tools that allow members of the public to see what others have reported online to save them having to report it themselves. This may allow the public to see incidents and issues already reported to us to save them time before deciding if they need to tell us something.

We are considering expanding our 'disclosure log' to include anonymised responses to enquiries as well as for requests where we think the substance of the enquiry would be of value to a wider audience.

Consultation

Over the coming months we will continue to consult extensively with organisations. As part of this, we will speak to businesses about their obligations, the opportunities any new data protection legislation may present, as well as how we should assist and inform them about the impact of any changes.

We started consulting at our GDPR implementation conference on 26 January 2016 with 100 delegates from business and public sector. The focus of this session was to discuss the impact of the new Regulation and how it can be implemented in a way that enables growth and innovation in business and delivery of public services. At our Data Protection Practitioner’s Conference on 6 March 2017 we ran panel sessions and workshops exploring and consulting further on the new obligations brought in by GDPR with 800 delegates in attendance and a further 4000 joining our live stream of the event.

The ICO recognises the need to engage with a wide range of organisations as part of this consultation, including SME’s and ‘challenger’ organisations. We also held a conference specifically aimed at SME’s in April 2016 which included a consultation with delegates about the implementation of the GDPR. We also acknowledge the need to look at the development of ‘safe spaces’ for organisations to develop innovative solutions to complying with the new rules. The outcome of this consultation will form a key part of the ICO’s innovation plans in the future.

Technology in the ICO

We are also using technology to maximise ICO efficiency. To this end we are:

Investing in a new telephony solution that enables efficient communication between all people and functions within the ICO, facilitates smarter working, is location independent, scalable and flexible. Where possible we use existing communications tools such as WebEx teleconferencing and FaceTime to facilitate engagement including international liaison with strategic stakeholders and partners.

Our intelligence team uses specialist software to map data flows in complex investigations. It uses dashboards to monitor progress of high profile and strategic files that require input from departments across the ICO.

We are also committed to using technology to enable our people to work flexibly and remotely, recognising that a modern workforce needs to work anywhere and at any time.

Conclusion

We trust that the above sets out clearly the ICO's commitment to, and recognition of, the importance of supporting innovation and growth through the use of new technology, both in supporting organisations and businesses in its use as well as in delivering our regulatory activities.