ico.
Information Commissioner's Office

[mark if sensitive]

Information Commissioner – induction briefing

Topic:ICO Strategic Planning

Author:Paul Arnold

Date of briefing:w/c 20 December 2021

Reference no:[will be provided to you in commissioning request]

Prepared for:John Edwards, Information Commissioner

Consultees:ICO Management Board

Reviewed/cleared by:Paul Arnold

For Commissioner use only- Follow-up required:

[A field for the Commissioner to use to include any initial thoughts on further follow up if required.]

ANNEX 1 –A paper considered by the ICO Management Board on 13 December proposing an approach to the development of our future strategic plan.

Briefing:

As you may be aware the ICO introduced an Information rights Strategic Plan (IRSP) at the start of Liz's term. Refreshed each year of Liz's term it has basically served as our overarching strategy for the past 5.5 years.

The IRSP was due to be reviewed and replaced in July 2021 at the end of Liz's term but we extended its life for a further year in light of the delay to your appointment. It will however need to be replaced by July 2022. This basically means we will want to consider and consult on its replacement in the first six months of your term.

Mindful of the need and importance of enabling you to inform this strategy we have held off doing too much preparatory work to date. We did however hold a range of internal workshops in May 2021 with our Heads of Service and Directors to consider what a fresh set of strategic objectives might look like. I was keen for us to do this work to help the leadership of the ICO focus proportionate attention on the post Liz ICO and to consider what our objectives might need to look like IF DCMS progressed their DP Reform policy proposals in line with expectations.

What I hope this now gives us is a useful platform on which to start developing our replacement for the IRSP. I have also spent a lot of time over the summer, including as part of my London Business School programme, considering how we might present our future strategy through the lens of a more compelling articulation of our 'purpose' as an increasingly complex regulator.

The paper I took to the Management Board last week brings things together. It includes my thoughts on purpose and includes the very much draft strategic objectives our workshops developed during the summer. I should stress that the draft strategic objectives would definitely require more development if we were to proceed with them. As a minimum we'd need to refine and sharpen the language in places.

What I'd like us to do John is discuss things as early as possible once you start. I would then like to take this work forward as soon as possible, capturing your thoughts and views as you settle into your role and making sure we have a draft strategy to take to our March Management Board meeting. This will involve supporting engagement with staff and DCMS as things take shape during January and February.

Annex - paper recently considered by ICO Management Board

Management Board - for assurance

Meeting agenda title:Future ICO Plan Implementation Proposal

Meeting date:13 December 2021

Time required:20 minutes

Presenter:Paul Arnold

Approved by:Paul Arnold

1. Objective and recommendation

To provide Management Board with a proposed road map for the development of the replacement of the current Information rights Strategic Plan. Subject to views from the Board, this proposal will then be put to John Edwards as part of his transition into role in January 2022.

2. History and dependencies

Earlier in 2021 the Board discussed our initial thinking for some possible enduring strategic objectives for the ICO. This latest paper builds on those discussions with our proposed next steps.

3. Developing a common understanding

The current Information Rights Strategic Plan (IRSP) was developed in 2016 and launched in 2017 with the intention that it represent the vision of the former Commissioner, guiding the work of the ICO for the duration of their term. It was therefore scoped to run to July 2021, with a new Commissioner expected to be in post by that point.

DCMS delays with the recruitment of the next Commissioner, and the corresponding request for Elizabeth Denham to extend her term, led to us extending the life of the IRSP. This was extended to July 2022 to allow for the continued uncertainty surrounding the timing of the start date of the next Commissioner and to afford time, post their arrival, for their thoughts and vision to inform the IRSP's replacement.

We now of course know that John Edwards will be the next Commissioner and look forward to welcoming him in January 2022. As well as needing to enable John to inform the way the IRSP's replacement develops (which we are proposing to call the 'ICO Plan’), we also need to build in time for consultation with staff and external stakeholders prior to July 2022. Our intention is therefore to capture the views of the Management Board prior to John's arrival in January to help to inform this process. We then propose for a draft ICO Plan to return to Management Board in March 2022 for further discussion prior to external consultation during the first quarter of 2022/23.

4. Matters to consider to achieve objective

As well as needing to develop new strategic objectives to guide the work of the ICO we should pause to reflect on the relative effectiveness of the IRSP as a plan/approach over and above its content. Whilst the IRSP has served us well as a strong statement of our ambition and intent during a period of major evolution of information rights law and awareness in the UK, there have been lessons learned:

- The IRSP set goals against which it was hard to measure the specific and unique contribution of the ICO. Most notably, the goal to increase trust and confidence in the way data is used. A stronger focus on tangible things the ICO is able to more directly inform and influence is therefore desirable for the future.

- We need our future plan to better articulate the choices we are making and intend to make when allocating our resources. The IRSP is ambitious, but it can also be used to support our work across a very broad waterfront. This means it can be hard to use the IRSP to inform our choices and provide direction to staff and clarity to stakeholders.

We are anticipating Government legislating to provide the future ICO with more explicit statutory objectives. Whilst these objectives are not expected to be in force until part way through the life of the future ICO Plan, where we are supportive of these objectives, we should align our ICO Plan with them. This will help us to develop the KPIs needed to enable us to account to Parliament for our future performance and provide greater clarity and continuity to stakeholders.

The ICO has a necessarily complex remit. We have statutory duties and obligations which, in some cases, are intentionally overlapping or carry an apparent tension between them. It is vital that we provide a clear explanation to our staff and stakeholders about how we believe these duties and obligations work together to form 'the purpose of the ICO'.

Under the IRSP we have struggled at times to do this. For example, how we balance duties to protect the public, support innovation and promote economic growth. To provide our staff with clearer direction and greater certainty to our stakeholders we should ensure that our future ICO Plan spends more time articulating our purpose and how our duties and obligations work together as well as setting out our separate enduring objectives.

Thinking more about our purpose

It has become traditional for organisations to strive for a short 'mission' and 'vision' statement to set the tone for their multi-year strategies and plans. Our mission and vision under the IRSP have been:

Our Mission: To uphold information rights for the UK public in thedigital age.

Our Vision: To increase the confidence that the UK public have inorganisations that process personal data and those which areresponsible for making public information available.

The challenge with this approach however is that the mission and vision often fail to describe 'why' the organisation exists and thus the 'purpose' behind which it wants its people and stakeholders to believe and invest.

In hindsight, we have also fallen into this trap with the IRSP. Our mission statement is describing 'what' we propose to do but doesn't explain why we believe it is necessary or important. In other words, it assumes everyone shares our belief and in so doing is only ever able to preach to the choir. When regulating in an area where there is not universal philosophical alignment with the regulator's mandate, or where there are significant new audiences to reach with complex messages, it is essential for the regulator to actively promote 'why' its work is needed.

Particularly for organisations with multi-faceted remits or controversial mandates, the challenge of the traditional mission and vision statements, even if they do capture the 'why', is also that they become so short and snappy that they fail to adequately articulate it with sufficient clarity for it to be understood or provide direction.

With particular reference to an organisation's workforce, there is considerable research supporting the view that greater empowerment, accountability, performance and of course engagement comes from people truly believing in their employer's 'purpose'. In other words, having a deep understanding of 'why' the organisation exists and their personal part in that journey. This goes beyond a more basic understanding of the organisation's objectives.

We know that many ICO staff join the organisation because they believe in what they understand to be the core purpose of the organisation. This emotional connection with our work is very powerful and should never be taken for granted. However, as the remit and mandate of the organisation continues to change and evolve, we need to make sure to take our people with us to avoid a mismatch between the story we are telling about our remit externally and the one our people believe in internally.

We have seen this healthy tension start to emerge to a degree in the past few years as we have increased our emphasis on innovation and economic growth. It is essential we ensure that our people and our stakeholders are helped to understand why we believe all parts of our mandate work together. It is not enough to simply say that we believe they do.

I believe very strongly that for the ICO to provide our staff and stakeholders with a purpose in which they can truly believe, and for it to be consistently understood by all, we need to take a different approach to explaining and articulating it.

Rather than trying to distil our purpose down to a couple of high impact 'mission' and 'vision' sentences or statements, I'd like us to develop a more comprehensive narrative which describes the 'why' of the ICO by truly explaining why and how we believe our various duties work together and the choices we intend to make when achieving our purpose.

This more comprehensive purpose statement will still only be a handful of paragraphs and it will incorporate our mission and vision. Whilst it may not fit on a bumper sticker, it should I hope be a much better way of engaging and empowering our people behind a clear and joined up purpose for the ICO.

The proposal is that this ICO purpose statement is the primary/top line means for John Edwards articulating and sharing his vision for the future ICO. We therefore propose to produce a first draft following initial discussions with John once he starts in role. We will then also seek John's views on the draft enduring objectives we'd then propose sit below the ICO's purpose statement. These are the draft objectives we developed earlier in 2021.

As also discussed earlier in the year, beneath the enduring multi-year objectives we will produce an annual ICO work programme which articulates our in year priorities and areas of focus. This will be informed by our annual strategic assessment.

Reminder of our draft enduring Strategic objectives:

Empowering and protecting people,particularly the most vulnerable, from the negative consequences of unlawful or irresponsible use of personal data.

We will help people understand how their data is used and how to exercise their rights, especially those that may be vulnerable.We will take effective and proportionate action against those that seek to use or obtain personal data irresponsibly or unlawfully.

Whilst recognising that we serve the public, we will also recognise that we have finite resources and are unable to look into every matter raised with us. We will seek and maintain our insight into the views and concerns of the UK public and use these to guide our priorities and allocation of resources.

Empowering and protecting businesses,creating a fair environment for those demonstrating good data protection practice by providing regulatory clarity to enable the responsible use of data to drive economic growth and taking action against those who try to gain advantage through unlawful or irresponsible use of personal data.

We will support businesses with our services and guidance to comply with data protection regulation – assisting them as they responsibly innovate, invest, compete and grow.

Data driven products and business models rely on individuals having confidence in how their personal data will be collected and used. We will support businesses to uphold trust in the data economy by providing better certainty; providing upstream advice and useful guidance and tools that reflect present practices. We will ensure that we are informing ourselves about latest developments in technology and personal data use so we can provide relevant services and viewpoints when they are needed.

We will recognise that organisations without routine access to specialist expertise, or those at the cutting edge of innovation, will need our help the most and we will prioritise our resources accordingly. We will not seek to cover all sectors ourselves but will work with regulatory colleagues to provide consistent advice and guidance through them where our regulatory jurisdictions align.

Cooperating and collaborating with our regulatory counterpartsto maximise regulatory clarity for organisations domestically, enabling the protection of UK data around the globe and underpinning the new UK transfer regime with effective regulation, tools and guidance.

By facilitating trusted international transfers of data, we will support businesses to access new markets – helping them understand and comply with overseas regulatory requirements and so expanding their opportunities to innovate, invest, compete and grow.

We will not invest in the development or maintenance of domestic or international relationships and networks which are not making a demonstrable and direct impact on our objectives. We will also ensure that any travel is proportionate and reflects the UK’s commitments on climate change, attending the majority of meetings, conferences or speaking events virtually rather than sending in person representatives where this is feasible.

Promoting openness, transparency and accountability, supportingthe development of the FOIA and EIR framework in the UK. We will oversee administration of the FOIA, supporting public authorities to be more open through advice, tools, practice directions and promoting proactive publication of relevant information and considering appeals escalated to us.

We will not continue to simply grow the approach of dealing with more and more appeals with static or net reductions in grant-in-aid funding but will instead focus on encouraging public authorities to be more transparent and open, publishing more information routinely and so avoiding the need for the public to escalate appeals to the ICO.

Enable the responsible use of data sharingto support effective data driven public services and data innovation. Helping organisations to understand how personal data can be shared responsibly and taking proportionate action against those that seek to share personal data irresponsibly or unlawfully.

We will not ‘authorise’ individual instances or programs of data sharing, as that is not our role but we will instead focus on creating a framework of advice and guidance so practitioners can share personal data with confidence and in so doing we will help tackle myths that data protection is an unhelpful barrier to data sharing and so undermines the safety of the public or acts as an unnecessary drag to innovation.

Effectively regulate cyber enabled data misuse. We will work with our partners to help organisations understand the threats facing the UK and to support them to take appropriate measures to keep personal data safe. We will supervise the cyber security of critical digital service providers and systems to protect citizens and business supply chains.

We will recognise the resources and role we have here. We are not the UK technical authority setting standards but will use standards developed by others (such as the NCSC and sector regulators) in measuring whether organisations have met their obligations. We will also not investigate every cyber incident but will instead focus on those posing the greatest harm to UK residents.

Continuously developing the ICO's capacity and capabilityto deliver impactful and credible regulatory outcomes and be recognised as an effective provider of public services, a knowledgeable and influential whole economy regulator and a great place to work.

We will ensure that we have the appropriate capacity, capability and culture to succeed and deliver impactful regulatory outcomes.

We will prioritise investment in resources which lead to the long-term evolution of our technical capability and workforce diversity. We will not simply grow existing non-technical capacities without challenging ourselves on whether demand led work pressures can best be addressed differently.

5. Areas for challenge

We know we are working to a tight timescale for this work. Ordinarily a new Commissioner would have nine months from arrival to the launch of their first full year plan. We do however need to be confident that the pace we are proposing to work at is feasible. This will be primarily be informed by John Edwards and his level of comfort with the direction of travel when he arrives in role, but views of the Board will be very helpful in stress testing the proposed approach at this stage.

6. Communications considerations

We will share this proposed approach with senior leaders during December. Wider communication will then be picked up by John Edwards as part of his first 100 days internal and external communications plan.

7. Next steps

The next steps for this work are:

- To reflect the views of Management Board in the proposal to share with John Edwards during December.
- To work with john Edwards to finalise the implementation programme following his arrival in post.

Author:Paul Arnold

ICO Digital and social media channels

Channel	Followers	Engagement (21/22)	Audience
Twitter: ICONews	80,919	2.32%	Mix of data protection/Freedom of information practitioners, media, tech industry and public (primarily 'political public' and those made complaints to ICO)
Twitter: Your Data Matters	2,301	1.34%	Data protection practitioners with some more general public.
Facebook	11,036	3.69%	SMEs, sole traders, public
LinkedIn	70,852	3.31%	Data protection professionals, Freedom of information professionals, legal, some SMEs
ICO e-Newsletter (industry)	217,906	30%	Data protection professionals, Freedom of information professionals, legal, SMEs, CEOs, marketers
ICO E-newsletter (public)	21,329	50%	Complainants, concerned public, data protection professionals

Website

Visitors (yearly)	Main traffic source	Popular pages	Audience
5,519,000 approx.	2,562,000 approx. via Google	The various news and blog content has had a combined view of 405,000 approx.	The website is accessed and contains content for all ICO stakeholders

Twitter

The ICONews Twitter account is our most followed social media profile. The account is verified and has the most varied audience with journalists, those from the data protection community, MPs and members of the public. The wide audience means it is our go-to account for disseminating information, such as public statements. It's also the most used social media account for responding to and advising the public on data protection/freedom of information concerns.

However, the often hostile or confrontational nature of Twitter means it is also where we receive some of our sharpest criticism. There are a number of data protection consultants and bloggers who use Twitter to comment on the ICO's policies and action. This is sometimes picked up by mainstream journalists for social comment and to inform news stories on their own platforms.

LinkedIn

LinkedIn is our fastest growing platform (+13% since Nov 2020). The account is mainly followed by data protection and access to information professionals. The audience's enhanced subject knowledge means we can go into more technical detail in our messaging, for example, with enforcement action we can explain some of the finer details of the breach and highlight the 'lessons learnt' for other users.

The more professional nature of the platform means we get less heated criticism. However, the criticism we do receive tends to provide more of an insight into debates or discussions into areas of contention or confusion amongst DP professionals.

We receive minimal queries via LinkedIn.

Twitter – Your Data Matters

This account was developed as part of the campaign to educate the UK about the GDPR in 2018. It is a public facing account and its aim is to educate and inform the public on their data protection rights.

It is the smallest account and has low engagement. The audience includes some members of the public, but also a number of the data protection community.

A challenge for this account has been a lack of content. We are looking to revive the account as part of our campaign work on our priority theme of "Protecting the Public" and are considering how best to do this.

Facebook

Our Facebook account has our largest "public" audience. Content aimed at educating the public on data rights, avoiding scams and any action taken against nuisance calls is very popular on this account. Any simple, small business guidance also performs well here.

We receive a high number of public enquiries on Facebook.

YouTube

We use our YouTube account as a hosting platform rather than a social media account. The content comes from webinars and conferences. We don’t monitor the account and don’t currently have any strategic aims to grow or use it for social purposes. Comments are switched off on the account.

Instagram and TikTok

We currently do not have an Instagram or TikTok account. Both platforms relies heavily on images and videos and success requires a significant resource commitment. But we are keen to review the opportunities (and consider the risks) of using these platforms as we move to our new team structure and operating model.

e-Newsletter

Our e-newsletter goes out monthly to more than 200,000 subscribers with ad-hoc emails sent on key topics, such as the launch of new guidance or to promote events. This is a channel that we can utilise more. In 2022, we will be updating our newsletter to include a new preference centre. This will enable subscribers to select the topics they’re interested in, which will allow us to send more relevant content to users.

Website

Our website is our primary digital channel. We post press releases, blogs and statements on the site. We also have comprehensive guidance on UK GDPR, the DPA, PECR, FOI and EIR. Our “Your Data Matters” section provides advice and guidance for the public. The site also allows us to build a number of interactive tools such as self-assessments and checklist.

The most engaged topics are

1. Data Protection fee (For orgs)
2. UK GDPR (For orgs)
3. How to access data (YDM - public)

4. Domestic CCTV (YDM - public)
5. SME hub

We are currently working to develop our website offering – from making guidance more accessible to creating a news centre that clearly sets out our news stories, our thought leadership (blogs and speeches) and our data/graphics/creative content.

Running a personal "Commissioner" Twitter account

John Edwards (JCE_PC) 7,435 followers

ICO (ICONews) 80.9K followers

Your Twitter account will be the first time a UK Information Commissioner has run a personal social media account whilst in office. This is a great opportunity for our communications but it is also worth being aware of some of the risks associated with this.

Opportunities

- **'Humanise the brand'**
  Having a named person behind an account or organisation helps to humanise the ICO and Commissioner role. It allows a space for personality and some commentary on issues from the your perspective / in the your voice, positioning you and the office as a thought-leader and enabling 'digital diplomacy' through constructive engagement with key stakeholders. We can help to grow your follow base.
- **Additional channel for ICO messages**
  It provides an additional verified account to share and amplify ICO messages and is a channel that can be considered in Comms plans.
- **Aligns with UK central government and other regulators**
  Ministers and Chief Execs of other regulators have a social media presence. Bringing the ICO in line would enhance perceptions of the

organisation as a modern communicator. Examples are included as Annex 1.

Risks/Considerations

UK social media culture can be very unforgiving and many high profile public figures have taken a cautious approach because of "cancel culture".

- **Unofficial posts being construed as "organisational view" or ICO policy**

  Your tweets have the potential to be perceived as the ICO view or as a suggestion of the ICO view and used by the UK media. This could apply to issues beyond data protection. There may be legal implications of publicly expressing some opinions while in office as a Corporation Sole, even if these are expressed in what is ostensibly a 'personal' capacity.

- **Previous posts**

  UK media have form of going through old tweets to try and find content that could be used critically (for instance - jokes that could be misconstrued or tweets that no longer have context).

- **Sub-tweets and perceived subtweets**

  Personal posts could be misconstrued and read as a view on a wider topic or as a "subtweet".

- **Retweets or shares seen as endorsements**

  Sharing an individual's post could be seen as a tacit endorsement of the individual and all of their other views.

- **Silence on issues**

  Whereas it would not be expected for the ICO to make a statement via our account or website to mark significant events or important days, the personal nature and "fast pace" of Twitter means that the your "silence" on matters may be criticised. Examples could include statements following national tragedies.

- **Twitter spats**

  Replies to criticisms online can easily spiral into a "Twitter spat", again this could be picked up by the media and used as an example of inappropriate behaviour by the ICO.

- **Freedom of information requests to the account would need to be considered**

  It is the ICO's view as the FOI regulator that it is best practice to consider any information requests to the account as valid requests. This would include any public tweets or direct messages (private messages). The ICO would need to consider how the account is managed to ensure that any requests aren't missed, to prevent reputational risk.

Recommendations

- **We work with you to review your account before your first day**

- We recommend updating the your bio to indicate you are the UK Information Commissioner, to direct enquiries to ICONews and to include a link to the ICO 'contact us' page.
- We recommend reviewing historic tweets should there be anything you want to remove.

- **You reduce or limit interaction with other Twitter users – particularly criticisms**

  Careful thought should be given to replying to users as criticism is unlikely to be resolved via Twitter and more likely to escalate.

- **The ICO should update its social media use policy**

This would outline how and why the ICO uses social media channels, codes of conduct around the channels and why and when we would block individuals.
Current social media policy here

- **Turn off direct messages feature for non-followers**
  This would limit private messages to only your own followers and therefore, reduce the number of potential FOIs received via your private messages.

- **You and your private office agree a process for managing the account and writing/posting tweets**

We recommend that:

- You retain responsibility for writing your content – adding value to the ICO's social presence through your voice, distinct from the ICONews account – but consider working with private office on posting.
- content is focused on ICO work, events and work-related engagement with allies and key stakeholders – which can be done in a timely way.
- tweets are posted when they have the best impact and engagement, and particularly around key events (for example, conferences or Parliamentary committees)

Retweets: it is a common practice for account holders to add a disclaimer that 'retweets do not equal endorsements' to their bio. Our recommendation is instead that content and content providers are checked for suitability before retweeting material.

- **You and your private office to agree a process for managing the assessment of FOIs**

  This includes both public tweets and direct messages.

- **Comms to develop advice for SLT/ET using social media accounts in a professional capacity**

Examples of good practice for Twitter use

- **Sharing "day in the life"**

  Lots of leaders share images and videos after events, this helps demonstrate the breadth and variety of their work. The ICO could do similar after you speak at events, media interviews 'behind the scenes' etc.

  Examples
  - Amanda Pritchard NHS Improvement
  - Emily Miles, Food Standards Agency

- **Adding additional perspective to ICO tweets and blogs.**

  Leaders often retweet and add an additional perspective to their organisations tweets and blogs. This adds the opportunity to add or emphasise a secondary key message, how work fits into the bigger picture or broader narrative and is another method of providing a spokesperson quote.
  - Amanda Pritchard, NHS Improvement
  - Nicola Dandridge, Office for Students
  - Lynne Owens, ex-NCSC
  - James Bevan CEO, Environment Agency

- **Digital Diplomacy**

  Tagging partners and key stakeholders to show ICO collaboration and influence to achieving shared goals.

Useful policies

- **ICO Social Media Policy April 2021.pdf**
- **GCS Propriety in digital and social media**
- **Speaker's Digital Democracy Commission: Recommended guidance for the use of Twitter by politicians - Members of Parliament and the House of Lords**

Annex 1 – assessment of regulators' used of social media

Regulator	Leader	Followers (to nearest 100)	Activity	Content
Charity Commission for England and Wales	Helen Stephens CEO	2000 followers	Very infrequent. No interaction with other accounts.	Charities with some personal
Ofqual	Ian Bauckham CBE, Chair	2300 followers.	Very frequent. No interaction with other accounts.	Education, events, lots of RTs.
Ofsted	Amanda Spielman, HM Chief Inspector	41k followers	Very infrequent. No interaction with other accounts.	Education and children

Office for Students	Nicola Dandridge	5,900 followers	Infrequent Minimal interaction with other accounts.	OfS work, education.
Environment Agency	Emma Howard Boyd, Chair	10.7k followers	Very frequently. No interaction with other accounts.	EA work, events, retweets of related work (ie views around COP26)
Environment agency	James Bevan, CEO	13.1k	Very frequently. No interaction with other accounts.	EA work, events, retweets of related work, media stories
Care Quality Commission	Kate Terroni, Chief Inspector Adult Social Care	2,800	Infrequently Occasional interacts with other accounts – work related.	CQC work, events and opinions.
Care Quality Commission	Ian Trenholm, CEO	2,700	Very infrequently. Occasional interaction	CQC work,

			with other accounts – work related.	
Health and Safety Executive	Sarah Newton, Chair	7,200	Frequently	
NHS Improvement	Amanda Pritchard, CEO	23.3k	Very frequently No interaction with other accounts.	Very professional –NHS work with some "national holiday posts" ie religious festivals.
Nursing and Midwifery Council	Andrea Sutcliffe, CEO	22k	Very frequently. Frequent interaction with other accounts on various topics.	Primarily NHS related, but with some personal tweets ie music interests, nature.
Ofcom	Melanie Dawes, CEO	5,000	Very infrequently. Minimal interaction with other accounts.	Tweeted more regularly whilst at MHCLG. Covered mix

				of personal with work.
Advertising Standards Agency	Guy Parker, CEO	1,000	Very frequently. Minimal interaction with other accounts	Primarily retweets without comment.
Food Standards Agency	Emily Miles, CEO	2,900	Frequently. Minimal interaction with other accounts.	FSA work, similar orgs work, events
NCA	Lynne Owens (previous Director General)	27.6k	Very frequently.	

Key Stakeholder engagement planning

This paper collates ideas for potential events based on your objectives identified so far, namely to:

- Identify key compliance issues for private sector organisations – in particular the service providers in financial and legal sectors
- Where is the compliance £ spent in resolving these issues?
- Insight gathering more generally
- External communications to show the Commissioner publicly in listening mode

The suggested events are not contingent on each other: we can for example arrange just one or two to cover the your priority objectives, or try to cover all of the objectives through combinations of events and methods such as online meetings, focus groups and surveys.

Aligning with our communications campaigns

Our external communications campaigns are brought together under four priority themes:

- Protecting the public
- Enabling innovation and economic growth
- Supporting the public sector to transform services
- Promoting transparency and accountability

A one-off listening exercise such as the 'business summit' outlined below, focused on compliance issues, would be most closely aligned with our theme of Enabling innovation and economic growth. It would enable us to demonstrate active engagement at the frontline and most senior level. A more expansive approach would represent a greater commitment for you and require corresponding investment of time and resources. However, it would help to mitigate the perception risk of an incoming Commissioner favouring specific stakeholders or stakeholder groups. It could also be positioned as supporting delivery against all four themes: a listening Commissioner capturing broad insights to inform the ICO's pragmatic and proportionate approach to its responsibilities as a whole-economy regulator.

Initial insight

To kick off the 'Events' programme for your first 100 days, we suggest a snap survey focused on compliance issues faced by organisations. We recommend that this should be available to all and promoted via social media channels. It can be pitched as tailored to larger organisations; however, by promoting it in our e-newsletter and via social media, we would enable all engaged organisations to give us their views. We could also widen the survey's focus.

The survey would serve a dual purpose: to gather some initial quantitative statistics through a simple series of yes/ no questions, and to function as a registration of interest to attend an upcoming event (which does not have to specified). Our suggestions for events held over the coming months are:

February 2022 – Business summit

Audience: Larger private sector companies

What are we planning? A 'business summit' including a meet and greet opportunity in person followed by pre-booked one to one short meetings which can be held over Teams, in line with social distancing requirements.

Who is it aimed at? Large private sector organisations. Relationship Management Service (RMS) are working on invite listing and key stakeholder contacts.

When do we propose to do it? Mid – late February. We can announce that you are hosting it in January.

1 half day (morning/afternoon) for the meet and greet.

2 afternoon sessions for the one to one session.

Where to we propose to do it? Central London / Teams

What are the main objectives? To gather insight from large organisations about their DP compliance requirements: Where is the compliance pound spent, and what are the key compliance issues being faced by the service providers?

March 2022 – Public sector round-table

Audience: Public authorities, charities, other

What are we planning? an informal meet and greet opportunity in person and a round-table discussion.

Who is it aimed at? Public sector organisations – Parliament and Government Affairs (PGA) and RMS are working on invite list and key stakeholder contacts.

When do we propose to do it? Mid-March

1 full day

Where to we propose to do it? Central London

What are the main objectives? To gather insight about DP compliance and FOI issues.

March 2022 – ICO Regions round-table

Audience: Various orgs based in UK nations

What are we planning: an informal meet and greet opportunity in person and a round-table discussion.

Who is it aimed at? Key stakeholders from various groups – Relationship Management Service and Regional Managers are working on invite list and key stakeholder contacts.

When do we propose to do it? late-March

1 full day

Where to we propose to do it? Regions – either Scotland or Northern Ireland are best fit. Comments from ICO Regions:

Scotland: We're likely to be taking enforcement action against the Scottish Government regarding aspects of the Scottish Covid app and this will obviously be high profile. There is a new Permanent Secretary starting in January and we should take up the opportunity for them to meet. Our new premises at Queen Elizabeth House has conference facilities we can use and so hosting a meet and greet would be simple to arrange.

NI: The only way to appreciate the ongoing impact of the Troubles in NI is to visit it. Much of our NI casework (both FOI and DP) is related to that history. We have an MoU with the Police Ombudsman (again, someone with a substantial Troubles-related caseload) just about completed and there would be an opportunity for the Commissioner to meet the Ombudsman. We'd also be able to facilitate a meeting with the new Head of the NI Civil Service – the last meeting Liz held with the previous incumbent led it to make changes to its approach to record management, which it has now had time to embed (we completed an audit of all departments in it earlier this year).

What are the main objectives? To gather insight about compliance issues.

Note: there is a data protection summit taking place on 24 March in Edinburgh. This will be a hybrid event and the ICO will be speaking. This might be of interest to the Commissioner to attend or tag on our event in the Scotland office.

The DP 2022 Summit will be held on 24 March in Edinburgh and online, will contextualise developments within the data protection field. The event will also provide an update from the ICO, looking at regulatory priorities; the Age Appropriate Design Code and anonymisation.

Conference topics include:

- Data Protection reform
- Information security and breach notification
- Databases, mapping and classification
- Global data flows and information sharing post Schrems II
- Anonymisation, pseudonymisation and encryption
- Impact of emerging technologies: AI, Cloud, Biometrics

Further information: https://www.dataprotection-summit.com/

April 2022 - Data Protection Practitioners' Conference – spring option

Audience: DPOs

What are we planning? The DPPC is the ICO's flagship annual conference, held fully digitally in 2021. Large hybrid event with keynote speakers and DPO workshops. Potentially an exhibitor hall.

Who is it aimed at? DPOs across all sectors

When do we propose to do it? Late April / Early May to tie in with the completion of the Commissioner's first 100 days.

1 full day

Where to we propose to do it? Manchester

What are the main objectives? To reach DPOs working in the field with new guidance and updates to policy, to maintain or work as active and relevant in public eye, to give DPOs the opportunity to talk directly to the ICO and its teams. An early chance for the Commissioner to share his vision and reflect on listening exercises.

May 2022 – Mixed online focus group

Audience: Priority audiences

What are we planning? Small focus group type event online.

Who is it aimed at? Cross section of attendees from young people / schools / older people who call the helpline / website users / SMEs.

When do we propose to do it? May

Where to we propose to do it? Online

What are the main objectives? To reach a broad relatively inexperienced public audience and gather insight into their issues and concerns about DP. We could look at more focussed interactions with some of these audience groups to tie in with our campaigns (e.g young people around the Age Appropriate Design Code or older women around our nuisance marketing campaign work)

June / July 2022 - Data Protection Practitioners' Conference – summer option

Audience: DPOs

What are we planning? As above: Large hybrid event with keynote speakers and DPO workshops. Potentially an exhibitor hall.

Who is it aimed at? DPOs across all sectors

When do we propose to do it? Late June / Early July. Can also tie in with the launch of the ICO's Annual Report.

1 full day

Where to we propose to do it? Manchester

What are the main objectives? As above, but potentially with a greater focus on the Commissioner's plan for the future of the ICO, informed by discussions with a broad cross-section of orgs in his first six months.

ico.
Information Commissioner's Office

Information Commissioner – induction briefing

Topic: Scheme of delegation introduction

Commissioned by: John Kavanagh

Priority: By 14 January

Owner: Louise Byers

Briefing aim: The objective of this briefing is to explain the scope and purpose of the ICO's Scheme of Delegation and to request that the Commissioner sign the current Scheme of Delegation to ensure continuity of delegated decision making.

List of Annexes:

Annex 1 – Scheme of Delegation for signature (separate document)

Context:

1.1. The Scheme of Delegation (the Scheme) is attached at Annex 1 to this briefing. This briefing is intended to give an overview of the Scheme to enable the Information Commissioner to sign the current Scheme and continue the existing delegations.

1.2. The Scheme is required because, as a Corporation Sole, all regulatory powers and responsibilities given to the Information Commissioner in UK legislation are vested in them personally. The Commissioner then needs to give authorisation to their staff members to exercise these powers. This is set out at Schedule 12, paragraph 6(3) of the Data Protection Act 2018 (DPA18). Without any delegations, the Commissioner would need to personally sign off on every regulatory intervention. The Scheme pulls together all of the delegations into one clear document.

1.3. Without delegated authorities being in place, any action that the ICO takes (such as providing advice or taking regulatory action) which is not personally signed off by the Commissioner would be *ultra vires*. The reason for asking the Commissioner to sign the Scheme this early in their term is to ensure the Scheme is up to date and reflect the appointment of the new Commissioner.

1.4. The version of the Scheme attached to this briefing was reviewed at the end of the previous Commissioner's term and signed by Elizabeth Denham. There are no substantive changes to the version that was signed by Elizabeth. This version also underwent legal review and was informed by advice from external Counsel.

1.5. The Scheme sets out every power that the Information Commissioner has in UK legislation. It provides a brief summary of what the power is, along with a link to the relevant part of the legislation (where possible) so that the full detail of the power is readily available. It then sets out the lowest level within the organisation to which the Commissioner has delegated authority to exercise powers. These delegations are subject to appropriate management controls regarding the allocation of work. Where possible, powers which are in multiple pieces of legislation (particularly the Data Protection Act 2018 and the UK GDPR) these are collated into one entry in the Scheme, to ensure consistency in the level to which these are delegated.

1.6. There are very few powers within the Scheme which are explicitly reserved only for the Commissioner. These are limited to approving the annual report and financial statements for laying in Parliament, laying other reports in Parliament, and appointing Deputy Commissioners. In addition, any powers that exist in legislation but are not included in the Scheme would need approval from the Commissioner to be exercised. We are not aware of any such powers.

1.7. For information, responsibility for the administration of updates to the Scheme sits with the Corporate Governance team. The next scheduled review of the Scheme will take place over August/September 2022. Ensuring adherence to the Scheme is a responsibility of all ICO staff, particularly line management within the areas that use the powers (particularly the Regulatory Supervision Service). The Legal Services Directorates provide legal advice on the Scheme, including engagement external Counsel for advice when necessary.

1.8. This briefing will be supplemented by a further briefing to explain how the scheme of delegation works with regards to the role of the

Information Commissioner in regulatory decision making, as well as the governance and decision making structures of the ICO.

Author: Chris Braithwaite

Date of briefing: 13 January 2022

Reference no: GP013

Prepared for: John Edwards, Information Commissioner

Consultees: John Kavanagh

Reviewed/cleared by: Louise Byers

Annex 1 – Scheme of Delegation – circulated separately.

For Commissioner use only - Follow-up required:

[A field for the Commissioner to use to include any initial thoughts on further follow up if required.]

ico.
Information Commissioner's Office

Commissioner Briefing

Date: 15 December 2021

Issue: Publication of the ICO's Draft Statutory Guidance (SG) & Regulatory Action Policy (RAP) for consultation

Key points:

- We will shortly publish an updated Regulatory Action Policy (RAP) and Statutory Guidance documents for external consultation next week; Elizabeth said she mentioned this to you in October.

- The aim of the consultation is to obtain views from both people and organisations who collect, use, store and share information about our an proposed updated approach to exercising our regulatory responsibilities and powers.

- Our existing approach was developed before the GDPR came into force and reflected the intense period of additional requirements being identified during later stages of the Data Protection Act being finalised. It was consulted upon at the time and approved by SofS and Parliament. It has mostly withstood the test of time well but we committed to keeping it up-to-date and it is now rather old.

- In updating the RAP and SG we need to reflect the changed situation post Brexit and reflect some learning from recent regulatory actions and appeals. Our preference is to update the documents now rather than wait a further 2 – 3 years for the Chandra changes to work through. The delays to Brexit, the Covid impact and then the DP reforms consultation have all already delayed earlier planned updates and we would prefer to avoid having such out of date material as our published regulatory position / process given the risk this poses to enforcement actions.

- We are proactively targeting a range of stakeholders to ensure we reach and obtain the views of a diverse audience. These include government departments, civil society, non for profit, industry, other regulators, and digital platforms.

- The changes to the RAP and SG are limited and focussed on ensuring the documents reflect our current working practices without prejudicing the outcome of the government reforms and this is reflected in the tone and content of our communications.

- To mitigate this, ET's view is that it is necessary and good housekeeping for us to publish an updated RAP and SG for external consultation prior to the DP reform outcome and legislation being passed . The RAP and SG both explain that they are a time limited product, and we acknowledge both will need to be reviewed, and where appropriate updated, to reflect the outcome and implementation of the data prospects reforms – likely from late 2023/24.

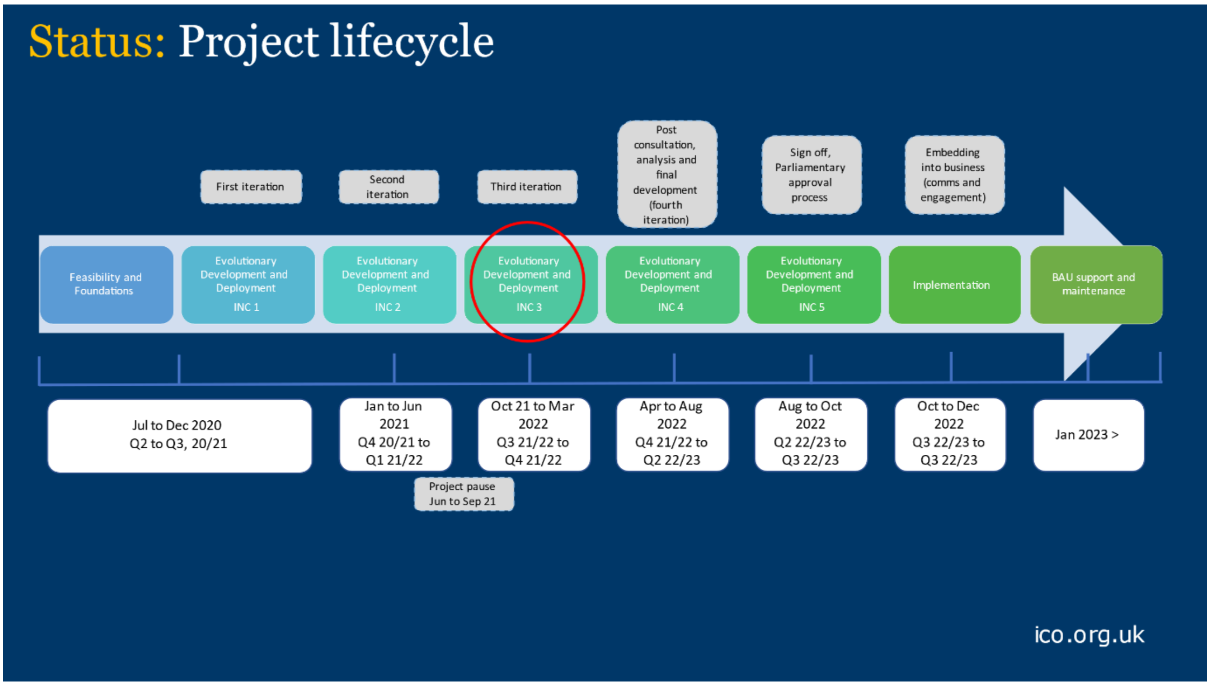
- The consultation is due to run for 14 weeks from late December 2021 to March 2022. A post consultation analysis will take place between April and June (subject to volume of consultation responses received). The final documents will be produced based on this feedback and shared with you for consideration and approval.

- The aim is then to table the SG with the Secretary of State for laying before parliament for their approval between August and October. DCMS are aware of the approach. The SG must be laid before parliament for 40 days. If no objections are made the documents will be formally listed as approved on Hansard and published on our website as final versions.

- As the RAP does not require approval from the Secretary of State it will, with your agreement, be finalised ready to be published once the SG is approved by Parliament.

- We can arrange an oral briefing with you in January to provide further detail if helpful. We will also build in time to include your views on our regulatory approach; it will provide a ready vehicle to implement any feedback you wish to act on following your stakeholder engagements.

Background info:



Status: Project lifecycle

First iteration

Second iteration

Third iteration

Post consultation, analysis and final development (fourth iteration)

Sign off, Parliamentary approval process

Embedding into business (comms and engagement)

Feasibility and Foundations

Evolutionary Development and Deployment INC 1

Evolutionary Development and Deployment INC 2

Evolutionary Development and Deployment INC 3

Evolutionary Development and Deployment INC 4

Evolutionary Development and Deployment INC 5

Implementation

BAU support and maintenance

Jul to Dec 2020 Q2 to Q3, 20/21

Jan to Jun 2021 Q4 20/21 to Q1 21/22

Project pause Jun to Sep 21

Oct 21 to Mar 2022 Q3 21/22 to Q4 21/22

Apr to Aug 2022 Q4 21/22 to Q2 22/23

Aug to Oct 2022 Q2 22/23 to Q3 22/23

Oct to Dec 2022 Q3 22/23 to Q3 22/23

Jan 2023 >

ico.org.uk

Author: James Dipple Johnstone, Chief Regulatory Officer

Prepared for: John Edwards, Information Commissioner

Topic: Developing our use of Artificial Intelligence (AI) and other related technologies

Purpose of report: To provide a high-level summary of the work we have delivered and are progressing in relation to the use of AI and other related technologies.

1. Linked to the Digital and IT Strategy 2022 to 2024

1.1 The evolving use of AI is a central theme in our developing Digital and IT Strategy that we are launching early in the New Year.

1.2 It reflects our ambition in this area to innovate and enhance the services we provide to both external and internal customers.

1.3 The current draft within the strategy is detailed below for reference:

"In its simplest form 'Artificial Intelligence' (AI) provides multiple opportunities for us to think differently in how we design and deliver smarter services. AI supports the imitation of the human mind like reasoning, problem-solving, planning, decision making.

It is primarily used to support intelligent decision making by considering the real-time scenario. An integrated AI service will read real-time data, understand the business scenario/logic and provide rapid outcomes. AI also has an extremely important part to play across the digital and IT service landscape and through wider learning and understanding, we will start to harness such capabilities in our service by design thinking. ICO has already realised some benefits in AI usage through the introduction of its 'Chatbot', and further learning from how our users interact with the solution will inform our future approach.

Some of the key benefits of AI include;

- Augmenting content creation by automating content management
- An enhanced customer service experience can be hyper-personalised through the influence of AI
- We can start to predict how our customers interact with us to identify trends and push out most appropriate content and guidance
- AI can decide the format of content and publish it automatically
- We can personalise self-help features based upon trend and usage to help reduce avoidable contact
- We can process huge amounts of data and information to help reduce the time taken to perform a task enabling multi-tasking and easing workload for existing resources"

2. AI Chatbot Scope

2.1 In September 2021 we launched a customer facing chatbot on the ICO Website within the section relating to organisations and specifically our DP Fees service - the link is - [Data protection fee | ICO.]()

2.2 Objectives of the Chatbot include:

2.2.1 Reducing the time visitors have to spend searching our website by leading them quickly to the answers and services they need in response to the queries they raise.

2.2.2 Act as a 'virtual assistant' delivering a more personalised service than we're currently able to offer outside 9-5, and that we can't always immediately provide during peak service hours.

2.3 The solution has been developed with the support of a third-party provider and our infrastructure is hosted within our Microsoft Azure Cloud platform providing an excellent level of resilience.

3. Current Performance

3.1 The chatbot is currently processing between 1,500 and 2,000 interactions per working day and circa 500 per day at weekends.

3.2 These interactions are split between "Enquiries" and "Conversations.

3.3 An Enquiry is a single question and answer, and a Conversation is multiple questions and answers.

3.4 The ratio currently between the two interactions is circa 50:50

3.5 Whilst difficult to exactly map impact on call volumes due to the current relative infancy of the tool, initial data suggest a reduction of circa 10% to 15% on calls due to customers being able to self-serve.

4. Ongoing Development of Services

4.1 Following successful launch within part of our public facing service we are currently evaluating the next phases of activity across other areas.

4.2 This focus is on areas of high transaction work which would benefit from automating a number of areas of enquiry such as our Public Advice and Data Protection Complaints Service.

4.3 In addition we have also very recently launched in November, a Robotic Process Automation (RPA) solution to our website, allowing users to change details such as address using a self-service tool that automatically updates our system without the need for ICO resources to process transactions.

4.4 Following go live we are processing circa 15% of requested changes via the RPA solution.

4.5 As we monitor the technical performance to ensure stability, we will further scale this up and increase traffic to this solution via increasing publication on our website and also our amending fee renewal letters to offer the online journey rather than an email address.

4.6 Similar to the AI solution described above, we are also evaluating other areas of our front-line services to ensure we maximise this new capability and offer our customers a range of options when accessing our services.

Author: Mike Fitzgerald – Director of Digital, IT and Business Services
Reviewed/cleared by: Paul Arnold - Deputy CEO and Chief Operating Officer

All staff briefing – Introducing the new commissioner

Suggested agenda:

1. Brief welcome to John and outline of the session – Jen
2. John introduction / opening remarks – John
3. Prepared questions – Both
4. Open questions – Both
5. Closing remarks – John

Prepared questions:

To kick start the session we've suggested 4 potential questions:

1. What are your first impressions of the UK and the ICO?
2. You'd shared in Twitter the kindness of strangers at Gatwick airport. I am sure that like me, many staff will be following your tweets. Whether that's a book review or your views on big tech – do you want to share some of your views about social media and how you use it?
3. I know that it's week 2, and so a little unfair to ask this of you, but what are your immediate priorities and areas of focus?
4. You've talked about a listening tour, whether that's with civil society, businesses and of course our ICO colleagues – what sort of questions do you have for us and how can we best engage and work with you?

Potential questions:

The following outlines potential questions you may receive from staff during the open Q&A.

There's 3 themes of questions, the first theme is about our work and your views about the approach you might take to it, the second is the ICO as an employer and again your views about that, and finally some potentially more personal questions about your achievements or where you plan to base yourself.

Likely questions from staff	**Implications / suggested answers**
Potential questions about our work:	
What is your view on the enforcement action the ICO takes? Should we be doing more or less? Will you be a carrot or stick Commissioner?	
What is your view of DP reform? Is this a positive review or will this dilute privacy in the UK?	
What's your views on FOI? Will you push to extend the law and for more money and resources?	
Have you hear about our complaint backlog? What are your views on this?	For information: There is a post covid-19 recovery plan in place and good progress is being made against that.
We know the consultation on international data transfers closed last year, what's your view on the privacy implications?	
How do you plan to work with government and parliament?	
We talk a lot about prioritisation of work. Do you plan to review the way we prioritise work? What are your immediate priorities?	
What changes do you want to make to the ICO? Will you change our structures? Do you plan to shake up ET?	
The constitution of the ICO might change meaning that we are no longer a corporation sole. Are you in favour of that change? What do you think that could mean for you personally or what are the implications for the ICO?	
From your previous perspective in NZ, what was the best or most impressive thing about the ICO?	

Likely questions from staff	**Implications / suggested answers**
Do you still think that Facebook isn't to be trusted? What are your views about our future relationships with the tech industry?	
As Commissioner, what changes would you like to see happen to the info rights landscape in the UK?	
People often find the balance of innovation and privacy difficult to find and some seem to think that it has to be one or the other, what's your view on that?	
Are you interested in adtech? Do you want to reinvigorate that work?	
You've said cookies don't pose a risk of harm. What would you like to see happen with the way we regulate cookie law/PECR?	
We know DCMS are pro-business and want to overhaul perceived DP barriers. Are you also pro-business? What is your view of this?	
You have experience of an "adequate" environment in NZ. Is there anything that concerns you with the current state of play in the UK in terms of maintaining adequacy?	
Regulating big tech is a constant challenge for us and other similar regulators. How do you think we should do it? Will you be pushing for more money and resources?	
We've had a lot of focus and resource on the Children's Code. Do you plan to continue that focus?	
Potential questions about the ICO as an employer:	
Car parking – we've been paying for it for two years and haven't used it. Can we have a refund?	Jen to answer – this is part of the Our Ways of Working programme and I'll update you on the review that's underway.
How do you plan to work with the Trade Unions?	

Likely questions from staff	**Implications / suggested answers**
We’ve been working at home for 2 years and the cost of utilities is rising dramatically, should the ICO pay for our heating?	Jen to answer – this is part of the negotiations with the TUs and Sarah Lal and her team can update you further.
What do you think about us largely working from home? What are the arrangements like in NZ compared to the UK?	
Potential personal questions:	
What do you think has been your greatest career success?	
Where are you going to be based? London or Manchester / Wilmslow?	
In social media, you seem to be a trans ally. Do you think this is an issue that the Information Commissioner should be outspoken about?	
We saw that you were pinged by test and trace. Did you have to isolate?	
Have you had a handover with Liz? Are you keen to see her priorities through or do you want to start afresh?	

Information Commissioner's Office

[mark if sensitive]

Information Commissioner – induction briefing

Topic: **DCMS UK Business Data Survey – points of ICO interest**

Commissioned by: Paul Arnold

Priority: Low, for info only

Owner: Emily Keaney

Briefing aim: Provide incoming Commissioner with market awareness of UK business sentiment towards data, provide incoming Commissioner with insight into the kind of business-facing research that DCMS as our sponsor department undertake as part of their data policy portfolio.

List of Annexes:

Annex 1 – Full text of survey https://www.gov.uk/government/statistics/uk-business-data-survey-2020

Body text:

Background

On 14 December 2021, DCMS published its UK Business Data Survey. It covers a wide range of territory, including awareness of the ICO and our guidance, awareness and benefits of GDPR and the DPA 2018, and some indicators of approaches to accountability.

It also includes analysis on where businesses get personal data from, whether they share it and/or use it for further analysis, whether they process sensitive personal data, including children's data, their approach to seeking consent, and their approach to transferring data internationally, including barriers and understanding of the legal framework.

Highlights

Awareness of/views on the ICO

44% of businesses have heard of the ICO and know what we do, 22% have heard of us but don't know what we do and 35% say they haven't heard of us. Sole traders are least likely to have heard of us and know what we do (40%) compared to large businesses (87%).

An estimated 55% of businesses that handle personal or employee data agreed (strongly or tend to agree) that they found the regulatory guidance published by the ICO clear and easy to understand. 80% of large businesses that handle personal or employee data tend to agree or strongly agree compared to 51% of sole traders and 59% of micro businesses

All businesses that handled digitised data were asked about the elements they felt required more clarity. These were:

- Lawful bases (42%)
- DPIAs (41%)
- Definition of special category data (40%)
- When data is anonymous (40%)
- What people's data rights are (38%)
- How and when to report a data breach (37%)
- International transfers (35%)

But there was a lot of variation by size, with large organisations most likely to say international transfers (53%) and micro businesses most likely to say DPIAs (43%).

<u>The benefits of GDPR</u>

An estimated 82% of businesses that handle digitised personal data said they either tended to agree or strongly agreed that they understand the requirements under GDPR and DPA 2018. Large businesses are more likely than small businesses to strongly agree: 73% of large businesses compared to 34% of sole traders and 39% of micro businesses.

Businesses that process personal or employee data were asked about possible benefits of the introduction of GDPR and DPA 2018. The three main potential benefits businesses highlighted were that it resulted in increased awareness of data protection at senior level (58%), increased accountability (44%), and improved awareness of data as a business asset (45%). However, nearly a quarter of businesses said there had been no benefits.

<u>Accountability</u>

Excluding sole traders, amongst businesses collecting digitised personal data, almost three quarters (73%) employ someone whose job role includes leading on data protection. The vast majority of large businesses (99%) and two-thirds (67%) of micro businesses have an employee in this role.

The majority (85%) of businesses that handle digitised personal data tend to agree or strongly agree to feeling confident that their business is complying with data subjects' rights under GDPR and DPA 2018 and 5% either tend to disagree or strongly disagree.

Almost two thirds (64%) of those businesses that process digitised personal data or employee data had a privacy management framework in place. This figure ranges from 59% among sole traders to 95% among large and medium businesses.

Author: Emily Keaney

Date of briefing: 15/12/2021

Reference no: CP047

Prepared for: John Edwards, Information Commissioner

Consultees:

Reviewed/cleared by: Paul Arnold

For Commissioner use only - Follow-up required:

[A field for the Commissioner to use to include any initial thoughts on further follow up if required.]

Information Commissioner – induction briefing

Topic: Information Access Performance

Commissioned by: Paul Arnold

Priority: Update as at January 2022, additional updates can be provided as required.

Owner: Louise Byers

Briefing aim: To provide an update on the recovery plan for the ICO's information access performance.

Summary

Information access performance is improving in line with the agreed recovery plan. Based on present performance, full recovery is forecast by the end of June 2022.

The recovery plan is based on a combination of reallocating existing, experienced, resources to our oldest cases and utilising less experienced staff from other departments to focus, with support, on new cases received. This approach has reduced the number of overdue cases while improving the timeliness of responses to new requests. Additional permanent staff are being recruited to maintain performance in the longer term.

Successful delivery of the recovery plan is expected to return us to our published service standard of 92% of requests responded to within statutory timescales. The standard we expect of the public authorities we regulate is 90%. Given the nature of the most complex and time consuming requests public authorities can receive we have always recognised that a 100% compliance rate would not be feasible for either the ICO or those we regulate.

Context

There has been a significant and sustained increase in information requests to the ICO over the last five years. This can, in part, be linked to the increased profile, complexity and impact of the work of the ICO as well as an increase in people's awareness of their information rights.

To put this in context, between 2017/18 and 2020/21 there was a 39% increase in information access requests received. There were 2,096 total requests received for 2020/21 compared to 1,509 in 2017/18.

During that time, we have increased the number of request handlers from 7.8 FTE in April 2017 to our current team of 17.4 FTE to deal with both the increase in volume and the increasing complexity of the requests we receive.

As well as increasing capacity, we have ensured our processes are robust and effective and, in order to provide assurance in relation to our request handling approach, an independent audit was commissioned in 2021. This audit, completed by Mazars, gave a 'green' or substantial level of assurance over the effectiveness of our processes.

We also continue to identify efficiencies within our case handling process, and have significantly increased productivity with the number of requests completed per month per FTE increasing from an average of 13.7 in 2017/18 to 19.6 in 2019/20.

However, from early 2020 onwards, the COVID pandemic saw a reduction in the capacity of the team without a significant drop in the volume of requests to the ICO. This meant that in 2020/21 we completed 84% of information access requests within statutory timescales. This was primarily as a result of the number of requests being completed per FTE each month reducing by 45% to 13.5 due to the impact of sickness absence and caring responsibilities.

The basic consequence of this dramatic and rapid reduction in capacity was an increase in the number of requests falling outside of the statutory timescale during 2020. At the height of the pandemic we did not manage to increase the capacity of the team quickly enough to rapidly return to our pre-Covid performance levels. A more fundamental recovery plan was therefore introduced and is being actively overseen by the Risk and Governance Board.

Recovery Plan

We have put in place a comprehensive recovery plan. Part of this plan addresses the overdue cases, through a 'late cases project'. This project has reallocated some of our most experienced request handling staff to deal with these overdue cases and the results of this can be seen in the reduction of the caseload:

- the percentage of the active caseload which is overdue has fallen from 37% (93 cases) in September to 23% (53 cases) in December and we expect this to continue to improve
- the project has also so far achieved an 81% reduction in the number of cases over 3 months overdue and a 43% reduction overall in our total late case backlog
- we also have a small caseload over 12 months old. This caseload has fallen from 13 in September to 4 in December and it is our aim to get this to 0 by end of February 2022.

The direction of travel and momentum of the recovery plan therefore remains positive.

To ensure that this focus on late cases does not adversely impact the service levels for new requests being received we have also temporarily redeployed a number of staff from other departments.

Although these staff are not experienced request handlers they are able to work effectively on our less complex requests with the support of our established core team. Because of the need to maintain a proportionate ratio between experienced request handlers and inexperienced temporary resource, we believe we currently have the optimal balance in place. However we will continue to keep this under review and if we are able to support additional resources to bring forward the timescales within the recovery plan, we will do so.

In acknowledgement of the longer term trend of increased demand, we have also created nine new permanent positions within the Information Access team to ensure we can meet future demand as our recovery plan concludes.

We have also been in communication with the regulatory department of the ICO, and have shared our approach and recovery plan with them, to provide assurance that our compliance is being actively addressed and prioritised. We will also be publishing our recovery plan on our website to provide greater assurance to the public regarding our future performance expectations.

We expect that delivering this recovery plan will allow us to achieve the requisite performance levels and to be back on target by the end of Q1 of the 2022/23 financial year.

Other points of note

We continuously review our request handling approach to ensure that we are improving. This includes considering how we apply exemptions and reviewing decision notices and case precedents to ensure our approach is as proportionate and as efficient as possible. Our work on proactive disclosure, working closely with regulatory and communication colleagues, is focussed on ensuring that we are publishing as much information as possible for the public and our stakeholders, thereby also reducing the need for requests to the ICO.

Author: Louise Byers

Date of briefing: 10/1/22

Reference no:

Prepared for: John Edwards, Information Commissioner

Consultees: None

Reviewed/cleared by: Paul Arnold

For Commissioner use only - Follow-up required:

[A field for the Commissioner to use to include any initial thoughts on further follow up if required.]

Responding to emerging technology

In this brief:

ico.
Information Commissioner's Office

Headlines

- Emerging technologies – including AI, advertising technologies, privacy-enhancing technologies and end-to-end encryption – are changing how personal data is processed. The **Technology Department** guides organisations on how data protection law applies to the use of these technologies and promote their responsible use.
- The legislative context surrounding these technologies is changing, with the Government proposing changes not just to the data protection framework but also new legislative measures on online safety and digital markets and a forthcoming White Paper on the Governance and Regulation of AI.
- Our analysis of these technologies is shaping the way that legislation is developed and informing shared positions with other regulators who govern these technologies. We also work with ICO regulatory supervision colleagues on audits and investigations where emerging technology is at play.
- The rapid development and convergence of technologies is creating an increasingly complicated landscape. Our ability to influence major technology firms and other digital players is contingent on technology skills and capabilities that we don't yet have or have not matured.

In more detail

1. Artificial intelligence

1.1. Artificial intelligence (AI) technologies are increasingly used to replace or augment human decision-making. In the vast majority of use cases these are powered by personal data, enabling automated decisions based on observed characteristics.

1.2. Good AI governance is needed to unleash the transformational power of AI while ensuring it works for people. Data protection issues include: ensuring transparency and fairness; tackling bias and discrimination; ensuring that people can exercise their information rights (e.g. to human review of significant decisions); and addressing emergent security risks.

1.3. In this context, the Government has announced plans to introduce a White Paper on the Governance and Regulation of AI in the first half of 2022, in parallel with the more imminent legislative reforms proposed in Data: a new direction. Other jurisdictions are similarly reforming their legislative frameworks, with the forthcoming EU Artificial Intelligence Act in particular expected to have an major impact on UK data controllers.

1.4. The ICO's Technology Department has responded to this context by:

- **Clarifying the requirements of the law**, by developing guidance on AI and Data Protection and Explaining Decisions Made With AI (produced in partnership with the Alan Turing Institute, the UK's national institute for data science and artificial intelligence).

- **Providing practical tools and advice** to support industry practitioners and the ICO's regulatory supervision team in their assessments of AI risks, for example through our draft AI and Data Protection Risk Toolkit and internal AI auditing framework. We work closely with regulatory supervision colleagues on audits and investigations where AI is a significant concern.
- **Collaborating with other regulators** to ensure a joined-up approach to governance of AI. This includes establishing a working group for all UK AI regulators to share information and collaborate as well as more in-depth work with the Competition and Markets Authority (CMA), Ofcom and the Financial Conduct Authority to forge integrated policy positions through the Digital Regulation Cooperation Forum. At an international level we work through the Global Privacy Assembly, Global Partnership on Artificial Intelligence and other fora.
- **Shaping the future legislative landscape**, by providing expert analysis on key AI and data protection issues to DCMS and its partner bodies, the Office for AI (a joint BEIS-DCMS unit responsible for overseeing implementation of the National AI Strategy) and Centre for Data Ethics and Innovation (an expert committee supporting the trustworthy use of data and AI). We have also provided input on the EU Artificial Intelligence Act, given its impact on the UK.

1.5. AI continues to be a hot topic, as its use and regulation shapes the lives of people across society. 2022 will see the ICO at the centre of work with government to define AI regulation, while influencing industry to build privacy-respectful AI and responding to calls for action from civil society.

2. Advertising technologies

2.1. Online targeted advertising drives the vast majority of the 'free at the point of use' web services, and is the major revenue stream for a broad range of publishers. It is also the revenue engine for Facebook, Google and increasingly Amazon, and has cemented Facebook and Google as gatekeepers in the online experience for millions of UK citizens, and billions of individuals across the internet.

2.2. The online advertising ecosystem is also a complex supply chain where the simple premise of an advertiser showing an ad on a publisher's domain can involve hundreds and sometimes thousands of organisations processing an individual's personal data. The level of personal data processing and sharing has allowed organisations to build highly intimate profiles of the movement and behaviours of individual across the web.

2.3. The Technology Department has responded to concerns about the adtech ecosystem by:

- **Conducting a market study into the Real Time Bidding (RTB) ecosystem**, to allow the ICO to assess the nature of the personal data processing taking place, and to identify any data protection issues. The analysis culminated in the 2019 ICO report into RTB which explored how the ecosystem worked, identified significant data protection issues, and set firm expectations for market participants around the changes we expected to see to address non-compliance.
- **Supporting Operation Cobar, launched in response to our concerns about non-compliance in the adtech industry**, by conducting technical analysis on cookie use and compliance with UK GDPR and PECR, and by acting as subject matter experts during audits by regulatory supervision colleagues.
- **Influencing emerging developments by the adtech market**, such as Google's plans to replace third party cookies with a set of new technologies (its so-called 'Privacy Sandbox'). Here, we have worked in partnership with the CMA, who have launched an investigation into the potential competition effects of Google's plans, to respond. We produced a Commissioner's Opinion setting out our data protection expectations for Google and other market actors, and influenced the CMA to ensure that the data protection impacts of Google's proposals are assesses as part of the legally binding commitments that Google has offered the CMA.
- **Spearheading work to replace 'cookie pop-ups' with more meaningful consent online**, building on our agreement reached with other G7 data protection authorities during the UK's 2021 G7 presidency. We are assessing what technical and policy changes are needed to ensure that browsers and IoT services can gather a user's choice, and ensure that any other service has to respect the choice. This approach has the potential to address concerns about 'click-through' consent mechanisms (dubbed 'the scourge of the internet' by some UK commentators), which add friction and fatigue to the browsing experience without yielding meaningful consent.
- **Shaping the future legislative landscape**, by providing expert analysis on cookies and similar technologies to inform DCMS plans to reform UK GDPR and PECR.

2.4. 2022 will see ongoing work with the CMA to shape the proposals by Google, the launch of the G7 cookies programme and potential enforcement action from the ICO in relation to RTB. In tandem, we will examine the role of other key players in the adtech ecosystem such as Facebook.

3. Anonymisation, pseudonymisation and privacy-enhancing technologies

3.1. Much data that is rich in potential remains locked in private and public sector organisations, leading to missed opportunities for growth and innovation. The

ICO has a crucial role to play in facilitating safe, legal and economically valuable data sharing, in line with the Government's National Data Strategy.

3.2. Anonymisation (processing of personal data to fully prevent the identification of the individuals the data relates to) and pseudonymisation (processing of personal data to prevent identification of the individuals the data relates to, unless additional information is used) are crucial techniques in helping organisations reduce the risks around data-sharing.

3.3. The rapidly-developing field of privacy-enhancing technologies (PETs) – such as homomorphic encryption, secure multi-party computation, differential privacy and privacy-preserving machine learning – can help organisations effectively pseudonymise or anonymise personal data. Despite the significant benefits, the development and adoption of PETs can be slow – with regulatory clarity needed on their application.

3.4. In this context, the Technology Department is:

- **Providing guidance on anonymisation and pseudonymisation**, to ensure data controllers and processors understand when data is personal data, and by introducing a 'spectrum of identifiability' framework to help controllers and processors assess the risks around data sharing. This will provide them with clarity around the technical and organisational controls they need to have in place to share data, and build their confidence in responsibly sharing data. The guidance is being produced in stages to solicit stakeholder feedback, and a formal consultation will be conducted in early 2022.
- **Promoting the adoption of novel privacy enhancing technologies (PETs),** through a series of techsprints with businesses wanting to share data and providers of PETs in early 2022. The project is backed by a £182,000 grant from the Government's Regulators' Pioneer Fund and will inform ICO guidance on the use of PETs, as well as increased communications and engagement to promote responsible data-sharing.

4. Biometric technologies and profiling

4.1. Biometric data represents the most intimate and immutable data related to an individual: you cannot, for example, change your fingerprint or DNA. The inappropriate or insecure use of such data can lead to substantial harms.

4.2. The value of such data in enabling identification and classifications of individuals is driving an acceleration in the development and use of biometric technologies, typically powered by AI. These include:

- the use of techniques such as facial, gait, vocal and DNA recognition for **identification** or **verification**
- the use of micro expression analysis, keystroke analysis and physiological sensors for **classification** and **inferences**

Novel use cases with potential privacy concerns are being identified in domains including employment, finance / insurance, transport, healthcare, education and law enforcement.

4.3. In this context, the Technology Department is:

- **Clarifying the requirements of the law**, by supporting the development of Commissioner's Opinions on the use of live facial recognition technology by law enforcement and by other entities, and on the use of age assurance technologies (which themselves may be necessary to support compliance with the Children's Code). The team also acts as subject matter experts during operations led by regulatory supervision colleagues.
- **Influencing emerging developments in biometric technologies**, with a foresight project established to identify emerging biometric technologies expected to have market impact on a 2-5 year timeframe; anticipate the associated data protection and privacy impacts; and deliver recommendations on how the ICO can address potential harms before they impact individuals, sectors or markets.

5. End-to-end encryption

5.1. End-to-end encryption (E2EE) is a technical measure that encrypts content in communications channels so that only the sender or recipient can access it.

5.2. Systems that do not use E2EE can be abused, creating the risk for financial fraud, exposure to harmful content and other harms. Real-life circumstances where the lack of E2EE has exposed people to harm include: children having their pictures accessed or location tracked, inappropriate access to medical data and collection of data for fraud and misuse.

5.3. However, because it restricts the detection of harmful content, E2EE also presents a challenge from an online safety and law enforcement perspective. The characteristics of E2EE that enable private and secure communications for the public also provide safe harbour for criminal activity. There are valid concerns that encrypted channels may create spaces where children are at risk.

5.4. In this context, the Technology Department has:

- **Undertaken a legal and technical analysis** of the requirements for E2EE in the UK data protection framework, informing the publication of a policy position on the governance of E2EE in response to requests from Parliament and other stakeholders. As part of this, we have engaged with key stakeholders representing all sides of the argument – including child safety advocates, privacy advocates, law enforcement, technology companies and other data protection authorities – to inform the ICO's position, and to identify opportunities to reconcile the competing objectives.
- **Worked with government and other regulators** to find ways to deliver on both online safety and privacy objectives. The Government has confirmed its support for strong encryption and that it does not support the

development of so-called ‘backdoors’ in social media platforms to allow access for law enforcement or security agencies. Through our Innovation Hub, we are supporting the Government’s Safety Tech Challenge that is investing in technological solutions, while through the Digital Regulation Cooperation Forum we are collaborating with Ofcom (the future online safety regulator) and other digital regulators to work towards joined-up policy positions on E2EE and content scanning more broadly.

5.5. 2022 will see continued debate on the balance between online safety and privacy with the passage of the Government’s Online Safety Bill (see brief on *Regulating the digital economy*). This will increasingly require the ICO to work with Ofcom to articulate joint positions on the governance of issues such as anonymous accounts and user ID; age assurance and profiling; algorithmic recommendations; targeted advertising; geolocation; and photo identification; as well as E2EE.

6. On the horizon

6.1. New technology and innovative business models can significantly change the scale, implications, and methods of processing personal data, catching regulators on the back foot. In recognition of this the Technology and Innovation Directorate recently established a Foresight team with a mission to:

> *“identify developments in technology and innovation in the mid-term (2-5 years) that impact data protection, advise the wider ICO on their implications and influence privacy outcomes.”*

6.2. The team is currently preparing a foresight report into the future of biometric technologies, but future reports could examine the data protection implications of the Internet of Things, neural interface technologies, distributed ledger technologies or immersive technologies (e.g. virtual and augmented reality). Further work is underway in the Technology Department to review data protection issues relating to cloud services.

6.3. Many of the key emerging technology issues will not necessarily be wholly new technologies, but the rapid evolution of existing areas of focus such as AI, privacy-enhancing technologies or biometric technologies and their application to new use cases (e.g. the use of AI in recruitment).

6.4. These thematic areas will often not be distinct, as technologies converge and combine (for example, AI underpins the development of age assurance and facial recognition technologies). Our challenge will be to assess the outcomes and impacts of these various convolved technologies, and decide on the intervention needed from the ICO.

6.5. The ICO’s ability to respond to these developments will require agility and investment to develop the technical expertise needed to scrutinise the data protection implications. This is one of the most challenging issues we face, with a buoyant tech job market often pricing the ICO out of attracting the tech talent we need.

Your first 100 days

7.1. We will work with you to identify opportunities for you to showcase the ICO's technology credentials early in your tenure. Scheduled announcements include:

- Launch of the ICO's **techsprints on privacy-enhancing technologies** in **February**, which will run until March and culminate in new guidance on anonymisation, pseudonymisation and privacy-enhancing technologies
- Publication of the final **AI and Data Protection Risk Toolkit** in **March**, following extensive consultation with stakeholders.

Your key stakeholders

8.1. Key stakeholders for the Technology Department include:

- **Government** – notably DCMS, the Centre for Data Ethics and Innovation (CDEI), the Office for AI (OAI) and the Regulatory Horizons Council (RHC)
- **Other digital regulators** – notably the Competition and Markets Authority (CMA), Ofcom, and Financial Conduct Authority (FCA) (see brief on *Regulating the digital economy*)
- **Major technology firms** – notably Google, Apple, Facebook and Amazon (see brief on *Regulating the digital economy*)
- **Technology representative organisations** – techUK, Coalition for a Digital Economy (Coadec) and the Centre for Information Policy Leadership (CIPL)
- **Tech think tanks and national institutes** – notably the Ada Lovelace Institute, Open Data Institute, Alan Turing Institute, Royal Society [*the national science institute*], Royal Society of Arts, Royal Academy of Engineering, Health Data Research UK
- **Technology standards bodies** – BSI [*the national standards body*], ISO, IEEE, and W3C
- **Civil society groups** – Open Rights Group, Privacy International, Which?

8.2. Your office is developing a programme of stakeholder engagement for your first days in post.

Your team

Stephen Bonner
Executive Director of Regulatory Futures and Innovation
Stephen.Bonner@ico.org.uk

Stephen Almond
Director of Technology and Innovation
Stephen.Almond@ico.org.uk

Ali Shah
Head of Technology
Ali.Shah@ico.org.uk

Supporting innovation and growth

In this brief:

Headlines

- The ICO's **Innovation Department** provides services to support innovators to engineer privacy considerations into the fabric of new ideas, products and business models – including sectoral outreach, one-to-one advice and in-depth testing environments.
- The "Innovation 2.0" project is reviewing how to maximise the impact of the ICO's innovation services in facilitating the introduction of privacy-respectful innovation. As part of this we are assessing the potential to introduce a fast, frank, feedback service for innovators needing data protection advice.
- The Government has proposed to introduce legislation that would give the ICO a new, more stringent duty to promote innovation and economic growth and remove requirements for organisations to consult the ICO on high-risk data processing. Enhancing and showcasing the ICO's innovation offer remains important.

In more detail

1. Supporting data-driven innovation

1.1. Data is powering the UK's economic growth. The data economy (data-driven goods and services) grew twice as quickly as the rest of the UK economy during the 2010s, making up c. 4% of UK GDP in 2020. With global volumes of data forecast to double between now and 2025, the opportunities continue to grow.

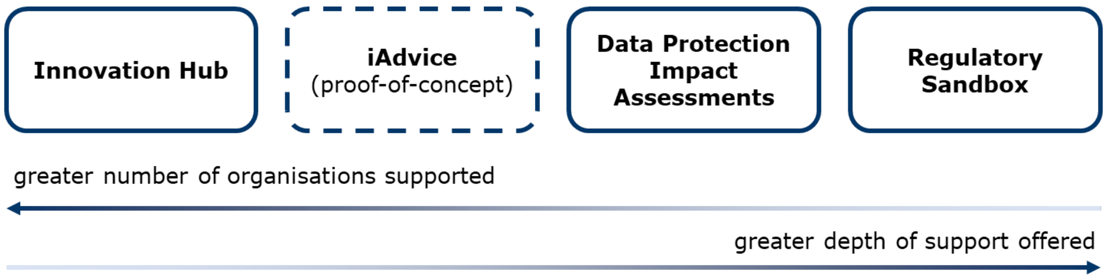
1.2. Personal data is at the heart of this opportunity: enabling the development and targeting of new ideas, products and business models that better meet people's needs. But to realise this potential people need to have confidence in how these new offerings use their personal data.

1.3. The ICO plays a crucial role in upholding public trust in data-driven innovation. The Innovation Department supports organisations to engineer data protection into the design of their innovations, with the aim of supporting privacy-respectful innovation to come to market and reducing the likelihood of future harm.

1.4. Innovative businesses are twice as likely as other UK businesses to seek regulatory information and advice. Where businesses face regulatory uncertainty, they are less likely to be able to persuade investors or consumers of the merits of their innovation – and less likely to introduce their ideas. Helping businesses develop privacy-respectful innovation is a key ICO priority.

1.5. With c. 1 million organisations regulated by the ICO, it is crucial that our support to innovators is targeted in a way that maximises our impact – reserving our most resource-intensive services for those organisations that are developing novel, high-risk propositions with potentially significant market impact. Our differentiated offer comprises four services:

Overview of the ICO's innovation services:


Innovation Hub
iAdvice (proof-of-concept)
Data Protection Impact Assessments
Regulatory Sandbox
greater number of organisations supported
greater depth of support offered

1.6. Our innovation services are designed to capture the insight that we gain from our engagement with innovators and use this to inform policy, guidance and communications to support all the organisations that we regulate, including through our Foresight team (see brief on *Responding to emerging technology*).

1.7. Supporting innovators isn't just a good idea – it's our duty. Under the Deregulation Act 2015, the ICO has a legal duty to have regard to the importance of promoting economic growth. In Data: a new direction, the Government set out its plan to legislate for a stronger duty on the ICO in regard to innovation, competition and economic growth, in recognition of the increasingly important economic role we play.

1.8. In autumn we established a project ('Innovation 2.0') to examine how we can maximise the impact of the ICO's innovation services in integrating data protection into the design of innovations and facilitating their introduction. The project will report its findings in spring 2022, which are likely to include recommendations for a substantial push on communications to position the ICO as a pro-innovation regulator and encourage organisations to engage with us.

2. The Innovation Hub: leading sectoral outreach to innovators

2.1. The Innovation Hub works at a sectoral level to help innovators build data protection into the design of their ideas and address perceived regulatory barriers to innovation. It does this by working through other organisations with a high degree of reach into specific sectors, such as innovation bodies or sectoral regulators.

2.2. Support offered through the Hub is tailored to each partner organisation and can include leading / supporting events for innovators and provision of data protection training to staff in partner organisations to help them guide the innovators that they engage with on privacy matters.

2.3. The Hub's work is targeted towards those sectors where there is a high degree of innovation in how personal data is being used. Current priorities include digital industries; financial services; health; smart cities; and legal services.

Sectors supported through past and present Innovation Hub collaborations:

fintech businesses through the **Financial Conduct Authority**'s Regulatory Sandbox and TechSprints

digital businesses through the **Digital Catapult**'s Machine Intelligence Garage

smart cities and related businesses through the **G20 Smart Cities** network and the **Connected Places Catapult**

medtech businesses through the **National Institute for Health and Care Excellence, Medicines and Healthcare Products Regulatory Agency, NHSX** and others

lawtech businesses through the **Solicitors Regulation Authority**'s Legal Access Challenge and **TechNation** LawTech Sandbox

3. iAdvice: providing fast, frank feedback on innovations

3.1. The iAdvice project is examining the feasibility and potential design of a direct advice service for innovators on the data protection implications of their novel propositions. It is backed by a £187,000 grant from the Government's Regulators' Pioneer Fund, which invests in experimental regulatory projects.

3.2. The service, if implemented, would complement and enhance the ICO's existing offerings to innovators by enabling them to get rapid advice on the data protection implications of their innovations: accelerating their journey to market. It would aim to work at high volume and fast turnaround and with less depth, with the highest-risk innovations handled by other services.

3.3. As with the ICO's other innovation services, the proposed service would gather insight on technology and market developments to help inform policy, guidance and communications and keep the ICO on the front foot. The proof-of-concept study will conclude in March 2022, with recommendations on whether to roll out the innovation advice service.

4. Data Protection Impact Assessments: reviewing high-risk propositions

4.1. UK GDPR created a new requirement to consult the Commissioner prior to introducing 'high risk' processing proposals where the controller is unable to reduce the assessed risk to acceptable levels. In this scenario, organisations are required to submit a 'data protection impact assessment' (DPIA) for 'prior consultation', with the ICO required to respond to these within specified timeframes.

4.2. Since the introduction of UK GDPR, we have advised on 17 prior consultation submissions. In roughly 1 in 4 cases we have had to issue a formal Warning, indicating that contravention of data protection law is likely should the proposal proceed as described. In all such cases, the organisations took steps to modify their proposals to prevent the identified contravention from occurring, allowing responsible innovations with real public benefit to come to market.

4.3. The team has also responded to more than 200 requests for advice on DPIAs that do not meet the 'high risk' threshold. Engagement on such proposals has enabled impacts on issues of high public importance, including influencing proposals for private sector use of facial recognition technology (leading to the subsequent development of a Commissioner's Opinion on private sector use of facial recognition technology) and shaping the design of COVID-19 contact tracing apps and COVID-19 certification schemes.

4.4. In Data: a new direction the Government proposed to remove both the requirement to complete data protection impact assessments (to be replaced by 'privacy management plans') and to undertake prior consultation with the ICO on 'high risk' processing proposals. We are considering how the DPIA function should adapt to accommodate any changes to the legislative framework and the potential introduction of the iAdvice service.

5. The Regulatory Sandbox: supporting testing of innovations

5.1. The Regulatory Sandbox offers the most intensive support of all the ICO's innovation services. Organisations must apply to work with the Sandbox team and are assessed on factors including how innovative the proposal is, the potential for public benefit and the alignment with ICO policy priorities (e.g. data sharing; use of novel technologies).

5.2. If accepted, organisations benefit from bespoke support for a fixed period during the development of their innovation. This can include workshops with design and development teams to inform early thinking; iterative steers as ideas move from concept to prototyping; informal supervision of product or service testing; and informal review of data protection documentation (e.g. data sharing agreements, privacy notices).

5.3. Organisations receive a statement of 'comfort from enforcement' for the duration of their participation in the sandbox and may request such a statement upon exit. Participation in the sandbox is reported transparently and an exit report published describing the outcomes of the project. Learning is captured and used to inform ICO policy, guidance and communications.

5.4. Seven organisations are currently participating in the sandbox, spanning projects ranging from supporting young people to access affordable finance through to developing AI-powered mental health services. An overview of past participants is found here.

6. Stimulating research and innovation

6.1. The Innovation Department doesn't just seek to support innovation to come to market – it also seeks to stimulate research and innovation that will improve privacy outcomes.

6.2. In 2016, it launched a £1 million grants programme to finance innovative research into privacy and data protection issues. It supports initiatives that contribute to raising public awareness of data protection issues and rights, promoting best practice and developing the ICO's own policy thinking in emerging areas of interest.

6.3. The eleven projects have covered topics including: the Internet of Things, data rights for homeless people, progress beyond cookies, and transparency in AI. For example, the grants programme funded research on children's attitudes towards privacy and their capacity to consent, which was used as a basis for the Children's Code. The third tranche of projects is due to conclude in early 2022, with the final tranche of projects due to complete by November 2022.

6.4. As the grants programme concludes, the Innovation Department is shifting focus towards areas where the market is failing to invest in innovation needed to deliver privacy outcomes. Gaps include the use of privacy-enhancing technologies – where the ICO's Technology Department is now running a series of techsprints with the support of a £182,000 grant from the Government's Regulators' Pioneer Fund – and the development of privacy-respectful 'safetytech' that keeps people safe online, where the ICO's Innovation Hub is supporting the cohort of innovators in the DCMS-led Safety Tech Challenge.

7. Promoting privacy by design

7.1. With c. 1 million organisations regulated by the ICO, we cannot hope to reach every innovator. In tandem with the services offered by the Innovation Department, we must ensure that our guidance is accessible to designers and engineers and helps them integrate privacy considerations at the product development stage, and so avoid data protection issues once services are active.

7.2. With this in mind, the Technology Department has pioneered the development of guidance that is targeted at designers, engineers and others who are developing services, rather than simply the legal and privacy compliance teams. The approach has borrowed from established norms for influencing product change within industry by offering clear reference designs for how to conform with the requirements of data protection, and by outlining our expectations.

7.3. Examples include the ICO's COVID-19 contact tracing app guidance, which provided app developers with a framework to test their designs for compliance with data protection requirements; the ICO's AI Risk Audit toolkit, designed to help organisations assess the data protection compliance of their use of AI; and supplementary guidance for designers and engineers on implementing the Children's Code transparency standard. The latter was co-designed with over 150 designers and engineers and won two industry design awards – a first for any data protection authority.

7.4. The ICO's pioneering work in this area is being emulated by other digital regulators, who are introducing frameworks to support safety by design, security by design and fairness by design. We are working with partners in the Digital Regulation Cooperation Forum to explore opportunities to integrate advice to developers and engineers.

7.5. We are developing plans to translate other areas of ICO guidance for a design audience. In tandem, we continue to foster an engaged community of designers and engineers that are seeking to apply the principles of privacy by design to their respective organisations – with a second Privacy by Design conference scheduled for 2022, building on our inaugural event that attracted over 400 technologists.

Your first 100 days

8.1. We will work with you to identify opportunities to set out your vision for data-driven innovation with the UK's technology and business community.

8.2. Scheduled announcements include:

- Conclusion of the DCMS-led **SafetyTech Challenge**, exploring ways to keep children safe online in end-to-end encrypted environments, in **March**.
- Conclusion of the **iAdvice** project in **March** and potential announcement of a new direct advice service for innovators in **April / May**.

Your key stakeholders

9.1. Key stakeholders for the Innovation Department include:

- **Government** – notably DCMS and the Department for Business, Energy and Industrial Strategy (BEIS)
- **Other digital regulators** – notably the Financial Conduct Authority (FCA), Medicines and Healthcare Products Regulatory Agency (MHRA) and Solicitors Regulation Authority (SRA)
- **Business and technology representative organisations** – techUK, Coalition for a Digital Economy (Coadec) and the Centre for Information Policy Leadership (CIPL), the Confederation of British Industry (CBI) and the Federation of Small Businesses (FSB)
- **Innovation funders, accelerators and representative organisations** – Nesta, Tech Nation, UK Research and Innovation, the Digital Catapult and the Connected Places Catapult
- **Tech think tanks and national institutes** – notably the Ada Lovelace Institute, Open Data Institute, Alan Turing Institute, Royal Society [*the national science institute*], Royal Society of Arts, Royal Academy of Engineering, Health Data Research UK

9.2. Your office is developing a programme of stakeholder engagement for your first days in post.

Your team

Stephen Bonner
Executive Director of Regulatory Futures and Innovation
Stephen.Bonner@ico.org.uk

Stephen Almond
Director of Technology and Innovation
Stephen.Almond@ico.org.uk

Lynne Currie
Head of Innovation
Lynne.Currie@ico.org.uk