Information Commissioner's Office

Response to DCMS consultation "Data: a new direction"

06 October 2021

ico.
Information Commissioner's Office

Foreword from Elizabeth Denham CBE, UK Information Commissioner

The opportunity to reflect on and review the UK data protection legal framework and regulatory regime is a welcome one.

Three years have passed since the introduction of the Data Protection Act 2018, and the pace and scale of innovation means the data landscape has changed significantly. How we deliver high standards cannot be static. Digital technologies are one of the engines driving the UK's economic growth. The digital sector contributed £151bn in output and accounted for 1.6 million jobs in 2019[1]. In June this year it was announced that the UK now has one hundred tech companies valued at $1bn or more, more than the rest of Europe combined[2].

It is important government ensures the UK is fit for the future and able to play a leading role in the global digital economy. I therefore support this review and the intent behind it.

As the proposals are developed, the devil will be in the detail. It will be important that Government ensures the final package of reforms clearly maintain rights for individuals, minimise burdens for business and safeguard the independence of the regulator.

> "Innovation is enabled, not threatened, by high data protection standards"

The energy powering these new technologies is our data: about our behaviour, our interests, our spending patterns, our loves and likes, our beliefs, our health, sometimes even our DNA – the very building blocks that make us who we are. The economic and societal benefits of this digital growth are only possible through earning and maintaining people's

[1] DCMS Economic Estimates 2019: Gross Value Added - GOV.UK (www.gov.uk)
[2] FINAL_TIGRR_REPORT__1_.pdf (publishing.service.gov.uk)

trust and their willing participation in how their data is used. Data-driven innovations rely on people being willing to share their data. ICO research shows that people who have heard about a data breach have lower levels of trust and confidence in all organisations using their data.

We need a legislative framework with people at its heart and I am pleased to see the consultation recognise the importance of maintaining and building public trust. It is crucial we continue to see the opportunities of digital innovation and the maintaining of high data protection standards as joint drivers of economic growth. Innovation is enabled, not threatened, by high data protection standards.

I support the intention of the proposals to make innovation easier for organisations. I agree there are ways in which the legislation can be changed to make it simpler for companies to do the right thing when it comes to our data. Perhaps most notably, it is vital that the inevitable regulatory and administrative obligations of legal compliance are proportionate to the risk an organisation's data processing activities represent. That means finding proportionate ways for organisations to demonstrate their accountability for how they collect, store, use and share our data. They must ensure data is safe and is not used in ways that might cause harm. And they must ensure that all people are able to exercise rights over their personal data.

> "An independent regulator assures the public of their protections"

To ensure high standards are met, and that people have the trust and confidence to contribute positively to the digital economy, the UK needs a strong, effective regulator. I welcome the proposals to ensure the ICO's powers are effective, and my office will be engaging closely with Government to ensure we have the resources we need to fulfil our role.

I also welcome the proposal to introduce a more commonly used regulatory governance model for the ICO. A statutory supervisory board with separate Chair and CEO will be better suited to the ICO's role as a whole economy and public sector regulator with extensive domestic and international responsibilities.

I welcome too the recognition of the value of an independent ICO. An independent regulator assures the public of their protections and maintains trust in data-driven innovation. By holding government and

public institutions to account, an independent ICO also builds trust in innovative uses of data in the public sector, and trust in democracy itself. And the independence of the regulator is key to the high standards that will help deliver future global trade and adequacy agreements.

Despite this broad support for the proposals to reform the ICO's constitution, there are some important specific proposals where I have strong concerns because of their risk to regulatory independence. For the future ICO to be able to hold government to account, it is vital its governance model preserves its independence and is workable, within the context of the framework set by Parliament and with effective accountability. The current proposals for the Secretary of State to approve ICO guidance and to appoint the CEO do not sufficiently safeguard this independence. I urge Government to reconsider these proposals to ensure the independence of the regulator is preserved.

> "I welcome the recognition of the value of our high data protection standards in international trade"

Recognition of the ICO as a strong, independent regulator is also important in how the UK is seen globally. As Chair of the Global Privacy Assembly I have seen first hand a clear trend towards high standards of data protection around the world. I welcome the recognition of the value of our high data protection standards in international trade. These standards make it easier to sell products and services. This is good for the public and good for business. Any reforms to the UK data protection regime should therefore always be weighed in terms of their impact on the ease with which data is able to flow between international jurisdictions.

> "A data protection framework that works for everyone"

The observations set out in this consultation response are based on our experience of dealing directly with how data protection law impacts people and business. My office has carried out a great deal of work to provide regulatory clarity to businesses through our extensive guidance and tools, as well as initiatives like our regulatory sandbox and grants programme. We also have strong insight into the concerns faced by the public and the regulatory challenges faced by small and medium sized

organisations through the hundreds of thousands of calls and enquiries our teams respond to each year.

Data protection is not just an academic exercise, or the province of regulators or data protection officers. It matters to all of us, and has the power to affect every aspect of our lives. I, and my office, remain committed to supporting the Government to ensure a data protection framework that works for everyone, and is fit for both the challenges and the opportunities ahead. The ICO has provided support throughout the development of these proposals, and stands ready to implement the reforms that Parliament decides upon.

Elizabeth Denham CBE
UK Information Commissioner

Contents

Executive summary

Our role in the consultation

The Information Commissioner's Office (ICO) welcomes this opportunity to respond to the consultation on future data protection reform. The ICO is independent from Government and responsibility for developing policy and for making changes to the legislative framework sits with Government and Parliament. Our role is to carry out the duties set out in the current, and any future, legislative framework and to provide expert advice to Government based on our experience of the current regulatory regime. This expert advice has been provided throughout the development of these proposals and we will continue to provide constructive input and feedback as the work progresses.

The importance of data protection

Data protection legislation is vitally important to all of us. It is grounded in human rights law and is designed to both protect and enable. High standards of data protection ensure the personal data we entrust to others:

- is kept safe;
- is not used in ways that we could not reasonably anticipate or expect, that would be unfair or cause us harm; and
- provides protections for those, like children, who are less able to control how their data is used.

Data protection legislation also ensures organisations are able to use, share and innovate with personal data responsibly. It holds them accountable for their practices, so we can all trust them with our data. The trust that high standards of data protection creates is key to delivering data-enabled social and economic benefits. It also facilitates innovation that allows the UK to thrive on both a national and international stage.

Our current legislative framework consists of the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (UK GDPR)[3], and the Privacy and Electronic Communications Regulations 2003 (PECR). The standards it sets out have been adopted into UK business models and are increasingly being incorporated internationally. However, the world is

[3] As incorporated by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019

moving quickly and we support Government's review of how the legislative framework and its regulation by the ICO could be improved.

Our engagement with stakeholders has also made it clear they welcome the certainty and seamless data flows with our major trading partners positive adequacy decisions provide, alongside the potential benefits of domestic legislative reform. This highlights the importance of ensuring any proposed reforms deliver specific and tangible benefits whilst safeguarding high standards of data protection.

The benefits of Government's proposals include the opportunities to support more data-enabled innovation and build on the platform the ICO has created for data innovation and regulation. We are already working to ensure data can be shared quickly, efficiently, and responsibly for the public good. We believe in reducing burdens on businesses, particularly small businesses, and agree there is more that can be done to simplify the rules.

We are looking to Government to ensure any changes to further support economic growth:

- retain high standards of protection for people's personal data;
- make sure people's data is used in ways that benefit rather than harm them; and
- make sure people can easily exercise their rights.

These are the foundations on which those wider social and economic benefits are built.

Enabling social and economic benefits

Data protection legislation is an important enabler of wider social and economic benefits. The role of data protection in the pandemic is a good example of where data protection was a key part of a trusted, responsible use of data in the Covid response. We particularly welcome the proposals to:

- **make it easier to use, share and re-purpose data for research (chapter one)**. We recognise the significant public benefit research can bring, when conducted with appropriate safeguards. This is reflected in our recent response to the Government's draft strategy, "Data Saves Lives: Reshaping health and social care with data"[4].

[4] ICO response-to-Data saves lives: Reshaping health and social care with data

Enhanced and sustained transparency and taking a data protection by design approach are key to achieving this aim;

- **introduce a statutory requirement for the ICO to have regard to principles including economic growth and competition (chapter five)**. We think this would help us support the use of data to deliver economic benefits for the UK, as long as this is done with appropriate protections; and
- **introduce a statutory requirement for the ICO to have regard to public safety (chapter five)**. Public safety is a primary responsibility of any government. We already work to support the appropriate and responsible sharing of data for the purposes of public safety. Our data sharing code[5] sets out examples of how organisations can do this. This includes where data needs to be shared in an emergency, or for the purpose of protecting vulnerable people such as in child protection.

Ensuring changes deliver for people

Given the importance of data protection to all of us, it is critical that the Government clearly and unambiguously sets out how its proposals would deliver for people, not just for businesses and society as a whole.

We welcome those proposals in the consultation that will enhance protections and control for people, particularly on cookies and nuisance calls. In both cases though we encourage Government to go further in order to bring greater benefits to people.

- **Removing cookie pop-ups (chapter two).** We agree the current approach does not work for people or businesses and welcome the commitment to improving this. Cookie consent mechanisms do not provide effective transparency or meaningful control for people. The information, and the processing to which it refers, is complex and most users click to accept without reading it. This is a consequence of the way in which the ecosystem has developed, with limited consideration of data protection requirements and underpinned by complex infrastructure. We would like to see a friction-free online experience, in which users' preferences about how their information is used and shared are respected.

[5] Data sharing: a code of practice | ICO

- The consultation's inclusion of the use of browser and non-browser based solutions is a good one. This is where people can say once how they would like their data to be used and have this respected across the online services they visit. This would allow people to choose to go pop-up free. However, to be effective there would need to be a mechanism for requiring organisations to respect these preferences, with appropriate sanctions where this is not the case. This is an issue that would require international cooperation to address. It presents an opportunity for the UK to provide leadership in digital regulation, including through our role in the G7. We would welcome further discussion with Government to ensure the ICO has the enforcement powers we need to make this solution work for people. This would ensure that those businesses that seek to do the right thing are not undermined by powerful online players who gain unfair advantage in the market by failing to respect user preferences.

  We also recommend that Government go further and consider the pros and cons of legislating against the use of cookie walls. This is where people have to 'accept' being tracked as the price they pay for being allowed to access and participate in an online service. This would reduce the incentive for organisations to put in place barriers that undermine how people have said they would like their data to be used.

- **Doing more to tackle unsolicited direct marketing calls and fraudulent calls (chapter two)**. This is a priority area for the ICO where we are already taking proactive action. We have called on successive governments to give the ICO more powers to tackle spam and nuisance calls. We are pleased that the National Data Strategy (NDS) is paving the way for these changes.

  We welcome the proposal to increase fines that can be imposed under PECR (which govern this activity) so they are the same level as those under the UK GDPR. We also welcome the proposal to allow the ICO to issue assessment notices to companies suspected of infringements of PECR, so we can carry out on-site audits of their processing activities. These changes would help us better investigate and reduce the harm caused to people by these often intrusive and distressing calls.

  We also think there is more that could be done, and would welcome discussions with Government about the potential benefits and costs

of aligning the whole of the PECR enforcement toolkit with that of the DPA 2018. This would allow us to take more effective action against companies that breached the rules. This would include issuing fines for breaches of PECR that are equivalent to those we can serve under the UK GDPR legislation. We think this could have an important impact on reducing the harm created by these calls.

Our strong support for these proposals is because of the clear positive impact we believe they will have on high standards of data protection, reducing unnecessary regulatory burdens on business, supporting fair competition and enabling the regulator to operate independently and effectively. The evidence for these positive impacts is clear in the proposals. However, we believe there remains more work for Government to demonstrate in sufficient detail how the remainder of the proposals achieve these objectives. In particular:

- **Removing the requirement to consider whether the legitimate interests being pursued by an organisation or third party when processing data are outweighed by the impact on the fundamental rights and freedoms of individuals (chapter one)**. This requirement is often referred to as the balancing test, and is used where an organisation is relying on legitimate interests as their lawful ground for processing personal data. It ensures organisations can use personal data in the ways they need to operate effectively. But only where this does not have an unwarranted impact on the rights and freedoms of the people whose personal data they are using.

  The consultation proposes creating an exhaustive list of types of data processing activities where organisations do not have to do this balancing test. The balancing test would not be needed because the Government would include only examples where the impact on people's rights would not outweigh the interests of the organisation seeking to use their data.

  We understand the desire to provide greater clarity and certainty in this area. Our understanding of these proposals is that they do not remove the need for an assessment of the balancing test. Rather they shift the responsibility for doing so from organisations to Government. Government would therefore need to be confident in drawing up such a list that the types of processing included in it do not have a disproportionate impact on people's rights. Parliament

would need to be similarly assured when passing any such list into law.

In order for Government and Parliament to have the required confidence, the nature, context and detail of the processing would need to be set out clearly. This is because these elements are central to determining the balance. This would also be important so that organisations could easily determine whether their own processing activities are covered by it. We are concerned that, as currently set out in the consultation, the types of processing are too broad to provide the necessary certainty. We are looking for Government to set out the nature of the specific types of processing in more detail, and how it has assured itself that those included in the list will not have a negative impact on people without the need for further case by case consideration of the balance at the point data is to be processed.

We would also welcome more detail on how this proposal will interact with the exercise of people's rights. For example, the right to object, where a data controller can only refuse a request if they have a compelling reason that overrides people's interests, rights and freedoms.

- **Clarifying the scope and substance of "fairness" in the data protection regime as applied to the development and deployment of AI systems (chapter one).** When people's data is processed, including when it is used to make decisions that affect their lives, both the process and the outcomes should be fair. This is particularly important in the context of AI, which allows for greater volume and complexity of data processing and where the risks of bias are amplified. We acknowledge that there is considerable complexity in this area, and welcome the intention to explore this further through the development of the National AI Strategy. However, we would be deeply concerned about any clarification or changes to the data protection regime that removed the centrality of fairness in how people's data is used. Data protection legislation should continue to ensure that when people's data is processed they are treated fairly. The ICO should continue to play a role in upholding that, working collaboratively with others, including other regulators, where appropriate.
- **Automated decision-making and data rights (chapter one).** We are concerned by the proposal from the Taskforce on

Innovation, Growth and Regulatory Reform (TIGRR) to remove the right to a human review of automated decision-making set out in Article 22, which is being considered as part of the consultation. Article 22 does not apply to all automated decision-making. It is intended to protect people where an organisation is carrying out decision-making solely by automated means, without any human involvement, where that decision-making has legal or similarly significant effects on them. These decisions are often made using AI. It requires organisations to:

- give people information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision; and
- carry out regular checks to make sure their systems are working as intended.

We welcome the consultation's focus on how to provide more clarity and guidance on what is a complex area. We think that could usefully include more guidance about what constitutes a legal or similarly significant effect, and the ICO is well placed to work with stakeholders to develop such guidance.

However, resolving the complexity by simply removing the right to human review is not, in our view, in people's interests and is likely to reduce trust in the use of AI. Instead, we think the Government should consider the extension of Article 22 to cover partly, as well as wholly, automated decision-making. This would better protect people, given the increase in decision-making where there is a human involved but the decision is still significantly shaped by AI or other automated systems. We also encourage consideration of how the current approach to transparency could be strengthened to ensure human review is meaningful.

- **Changes to subject access requests (chapter two)**. Subject access requests (SARs) refer to the legal right to ask a company or organisation for access to the personal information it holds on you. Organisations can use this information to make decisions that have a major impact on people's lives. SARs therefore deliver fundamental data protection rights of transparency and access to personal information. They have been in existence since before UK GDPR and are referenced in the requirements of Convention 108+[6],

[6] Convention 108+ was signed by the UK in 2018 and is awaiting ratification.

the successor to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

Subject access requests are key to exercising other data protection rights. This right is even more important as many of the reforms set out in this consultation encourage the increased collection, use and re-use of data. This is likely to mean the number of organisations holding data about us, and using it to make decisions about us, will proliferate.

The largest proportion of complaints the ICO receives from the public are about SARs, with 46% of complaints focused on this issue in 2019/20[7]. We welcome the recognition in the consultation of the importance of SARs in delivering data protection rights. We also recognise that responding to some subject access requests can require significant resources for some organisations. However, it is vitally important that more evidence is gathered from relevant sectors to assess the benefit and risks of any changes to this right. This includes assessing the proposed introduction of a nominal fee and cost limit in order to avoid disproportionate outcomes for people, particularly the most vulnerable. If changes are made they must come with safeguards to ensure that everyone, whatever their circumstances, is able to exercise this right. We would also like to see more detailed consideration of how any safeguards would work in practice and how any potential equality issues in this area would be addressed.

- **Prior consultation with the ICO on high-risk data processing (chapter two)**. In some cases organisations may identify that their processing poses a high risk to people that they are unable to reduce. At the moment, they are required to consult with the ICO in advance of that high risk processing taking place. The ICO does not receive large numbers of these requests, indicating that that the provision does not currently represent a significant burden for business. However, the process does create an opportunity for the ICO to provide early and effective advice to organisations engaging in the most high risk processing, giving assurance and support to innovation. It also ensures we can work with those organisations to mitigate harm to people before it happens, which is what we believe the public expect. We agree there is scope to reform the current

[7] Information Commissioner's Annual Report and Financial Statements 2020-21

approach, but rather than remove the requirement we recommend introducing a more agile and flexible threshold for when prior consultation is required. This would better reflect emerging risks and public concerns. Reforming the threshold would also better support organisations to identify the kinds of risks where they would need to consult with the ICO in advance. We also recognise the importance of any requirement for consultation to be proportionate and risk-based.

Removing the threshold would reduce our ability to prevent people experiencing harm, restricting our role to taking action after that harm has occurred. An unintended consequence could also be that the ICO will need to fall back on its formal investigative approach to address any potential harms from such processing. This proposal would therefore not be good for businesses or public service innovation. It reduces regulatory certainty and, if businesses or public service initiatives end up retro-fitting privacy measures rather than designing them in at the start, it could undermine public confidence, damage reputations and increase costs.

- **Proposals around data re-use and data re-purposing (across the consultation).** There are a number of proposals in the consultation that would enable greater re-use or re-purposing of data. While individually these proposals could bring benefits, it is important to consider the collective impact of the proposals, which taken together could increase the re-use of people's data in ways that they may not anticipate or expect.

Ensuring organisations are accountable

We are pleased to see recognition in the consultation that accountability is a critical element of data protection regulation and implementation. Businesses and government now have access to huge volumes of our personal data. They use this in ways that have a significant impact on our lives. Ensuring they are accountable for using data responsibly and keeping it safe is crucial.

We therefore welcome the intention in the consultation for Government to **explore options that would better support certifications as an alternative transfer mechanism** (chapter 3). Both certification schemes and Codes of Conduct are types of voluntary accountability tools that provide organisations with the means to take ownership for driving up standards and ensuring compliance across their sectors. They are a

valuable and currently underused tool that could bring value both in the context of international transfers and more widely.

We welcome the proposal to **require an organisation to try to resolve complaints before they are referred to the regulator** (chapter 5). This would encourage organisations to take responsibility for getting to the bottom of complaints before they come to the ICO, making it quicker and easier for people to get their complaints resolved. It would reduce the regulatory burden for organisations, as they would be significantly less likely to need to engage with the regulator on their handling of complaints. It would also mean the ICO could focus on cases where intervention was most necessary, ensuring efficient use of resources that deliver the best outcomes for people and businesses.

We also welcome the proposal to **introduce a proportionate requirement for organisations to report on the nature and volume of complaints they receive** (chapter 5). This would enhance transparency and is a positive tool to drive market led compliance. To further enhance the effectiveness of the proposals on complaints, we would recommend Government consider giving the ICO the power to make recommendations to a data controller about how best to resolve a complaint. This would ensure complaints from the public lead to tangible outcomes, which is often what they tell us they want when they come to us for help.

The consultation talks in detail about how to revise the approach to **ensuring organisations are accountable and are able to demonstrate that accountability (chapter two)**. It proposes a new approach based on risk-based privacy management programmes. Or, if the Government decides not to pursue this approach, a number of smaller suggested changes to the current accountability requirements. We welcome the Government's commitment to ensuring the UK's data protection regime retains the principle of accountability at its heart and are open to alternative approaches to ensuring accountability. Whatever approach is taken, it is crucial to retain in law the requirement that organisations should be both accountable and able to demonstrate accountability. We are keen to build on the progress made through the ICO accountability framework[8], which we have consulted on extensively.

We think more work is required to demonstrate the additional value that PMPs would deliver. Any substantial change to the approach to

[8] Accountability Framework | ICO

accountability would bring potential disruption and could create a burden for business. We know many organisations have put significant resource into developing their approach. Any changes should not create an additional burden for them. We therefore welcome the fact that the proposals for introducing a privacy management programme include provision for organisations to be able to demonstrate compliance using the approaches and processes developed to comply with the existing law. However, we also encourage Government to continue to explore whether the benefits they are seeking to achieve through introducing PMPs could be achieved with more minor changes to the current accountability requirements.

It will be important to consider evidence from organisations about how they could evolve from their existing approaches to accountability to the PMP model. Smaller organisations in particular would require more digital tools and support, which the ICO would expect to provide. But there would need to be time for transition and adequate resources to do it effectively.

Within both approaches, there are several specific proposals, including **removing or amending the requirement to appoint a data protection officer (DPO)**. We agree that it is reasonable for organisations to assess the most appropriate way of assigning responsibility for data protection compliance within their organisations. The current requirements for appointing a DPO are overly prescriptive and can be challenging for organisations. However, the introduction of DPOs has brought significant experience and professionalism to data protection compliance. This professionalism is a valuable asset to organisations. We would like to see it developed and supported, with a focus on the outcomes and value these roles can deliver. We also note that appointment of a designated role to undertake important compliance functions is a common approach that brings both expertise and assurance in many sectors, including in finance and health and safety.

It is important that the independent advice, skills, leadership and links to board level governance brought by DPOs are not lost as a result of any changes. The consultation proposes requiring organisations to designate a 'suitable' individual, stating that they should have discretion to consider the skills, qualifications and position needed for the role. While this is welcome, we also encourage Government to consider more widely how to retain the value and expertise of those roles. This is particularly relevant in organisations with the highest levels of data use and consequently the

highest potential risk to people, where having a dedicated role with responsibility for ensuring people's data is properly protected is an important safeguard.

There are also proposals to **remove the requirement to conduct a data protection impact assessment (DPIA)**. This would be replaced by a more general requirement to have assessed and appropriately mitigated the risks arising to people from the data processing. DPIAs are an important tool to help organisations understand and manage these risks. During the Covid pandemic DPIAs have been invaluable for controllers to understand the breadth of data protection issues quickly and efficiently, while taking action to protect the public. We agree that there is scope for more flexibility about the form that these assessments take. However, it is important that this does not result in a reduction in the robustness or quality of those assessments related to risk.

Whatever form the assessment of risk takes, it is important the Government retain a reformed requirement to consult the regulator about the impacts of high-risk processing. As noted above, this is an important protection for people, as well as supporting organisations to innovate responsibly.

We also note the proposal to introduce a new **voluntary undertakings process**. This would mean an organisation able to demonstrate it has embraced a proactive approach to accountability could provide the ICO with a remedial action plan upon discovering an infringement. The ICO would be able to authorise this plan without taking any further action, provided it met certain criteria. If introduced, it would be important that this approach would not reduce our ability to use our regulatory discretion to:

- make a judgement as to whether to accept a remedial action plan as sufficient; or
- take action based on all the circumstances, even where an effective management plan is in place.

In such a system, the ICO would also require access to and information about an organisation to assess its compliance with a voluntary undertaking. It would also need to be clear this would only be an option where an organisation proactively raises the infringement. It should not be an option to avoid a sanction following an ICO investigation of an infringement.

We support the proposal **to introduce compulsory transparency reporting on the use of algorithms in decision-making for public authorities**, government departments and government contractors using public data. We welcome this approach and agree it is currently challenging for people or their representatives to understand:

- how AI systems are being used;
- how ethical considerations such as mitigating bias have been addressed;
- the approach to human oversight; and
- the level of risk associated with the algorithm.

We think this proposal would help provide scrutiny over and accountability for the use of this data in the public sector. We encourage Government to consider how proactive publication mechanisms within the Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations 2004 (EIRs) could be used to support the implementation of proposals in this area.

We think Government still needs to provide more detail on the proposals to allow organisations to use data more freely by **developing a safe regulatory space for responsible development, testing and training of AI**. This kind of approach can be extremely effective. The ICO already operates an internationally respected regulatory sandbox to support the testing and trialling of new ideas, products and business models, including those related to AI. However, using AI for processing personal data can often be high risk for people. It is therefore important that there are appropriate safeguards in place to manage risk and prevent harm. More detail is needed on these and on the proposed role of the ICO. The ICO's involvement would both ensure effective safeguards and provide organisations with the regulatory certainty to develop their approaches with confidence.

The UK's international role

While we now have the freedom to adapt our laws to suit us, data protection legislation does not operate in a vacuum. It is important to ensure the UK's data protection framework continues to be aligned with the wider international move towards locking in high standards of data protection, such as those set out in Convention 108+. The UK has excelled at setting high standards and many of these are now being adopted globally. Any reforms need to reflect this to ensure the

continuing confidence of the UK public, support the UK's global influence and enable UK businesses to compete globally on a level playing field.

Organisations also need to be able to transfer data internationally in ways that facilitate the real-time flows of data in the digital economy. At the same time, the public expect that their data is protected to a sufficiently high standard. It is important any reforms in this area ensure organisations are able to employ risk-based, practical approaches to balancing these requirements. We welcome the discussion of possible approaches to supporting organisations to do this easily and safely (chapter three).

This is an area where the ICO has been taking proactive action. We have recently published our approach to replacing standard contractual clauses with a proposed International Data Transfer Agreement and Transfer Risk Assessment[9], along with new guidance. As part of these proposals, we are seeking to take a risk-based approach that will be more usable for SMEs. We look forward to hearing what more stakeholders would value in this area.

Maintaining an effective and independent regulator

Ensuring data protection legislation delivers high standards of protection for people, enables wider social and economic benefits, and holds businesses and the public sector to account requires a strong, relevant, independent and accountable regulator.

We welcome the proposals in the consultation to **strengthen our supervision and enforcement powers (chapter five)**. These amendments would ensure we are able to use our powers appropriately and proportionately to protect people and create a level playing field for compliant organisations. They are in line with the powers of other comparable UK regulators and address gaps we have identified as we operate under the existing legislative structure.

The recent Government commissioned TIGRR report advocates delegating greater flexibility to regulators to help them regulate in a fast-moving world. It also argues for increased accountability and scrutiny of regulators as a counterweight to this increased autonomy. This is also

[9] Consultation on data transferred outside the UK: ICO consults on how organisations can continue to protect people's personal data when it's transferred outside of the UK | ICO

discussed in the recent BEIS consultation "Reforming the Framework for Better Regulation"[10].

We agree that independence and flexibility to regulate in a way that allows us to hold both government and businesses to account and respond to a rapidly changing external context are crucial. In a democratic society this must be done within a framework of strong accountability. This is a key feature of the internationally respected UK regulatory model and builds public trust, as well as supporting good governance. We are therefore supportive of many of the proposed changes to the governance and accountability of the ICO (chapter five). Many are informed by work already underway at the ICO to align with corporate governance best practice. It is important that as a public body we are accountable to Parliament and Government and **we support clear statutory objectives for the ICO and a clear parliamentary articulation of the ICO's regulatory framework**. The requirements to uphold principles such as economic growth, competition, public safety and regulatory cooperation build on our existing work.

However, some of the proposals risk undermining the independence we need to carry out our responsibilities under both data protection and freedom of information legislation to oversee government and the public sector. Independence, within a framework of strong accountability to Parliament, is important. It allows us to regulate without fear or favour, to make decisions about where we intervene or act based on an impartial assessment of the harm or potential harm to people. It also reassures the public that our actions are impartial and that government as well as businesses are being held to account. This builds the trust needed for people to be willing and engaged participants in the digital economy. The independence of the regulator will also be an important element in securing future global trade deals and adequacy agreements.

Giving the Secretary of State the power to approve or reject codes of practice and complex or novel guidance (chapter five) would reduce the ICO's independence. It would also reduce regulatory certainty for organisations and wider trust and confidence in the ICO's guidance. It could also lead to more legal challenges, such as judicial review. In such challenges it would need to be clear who the respondent would be in the context of a challenge to guidance that the Secretary of State had determined. It is our belief that, as an independent regulator, the ICO should be able to issue its own guidance, with a commitment to

[10] Reforming the Framework for Better Regulation: a consultation (publishing.service.gov.uk)

take account of the views of stakeholders and the impact on economic growth.

As well as reducing our independence, this proposal also reduces the ability of government to effectively hold the ICO to account. We expect and need government to maintain the ability to hold independent regulators to account for the consequences of the products they produce and decisions they take. This is made more challenging if government is the final approver of the guidance and products which establish the standards of legal compliance and regulatory certainty for stakeholders.

The proposal for the appointment of the Chief Executive (chapter five) does not sufficiently protect the ICO's independence. We believe this appointment should be made by the ICO Chair and Board, in consultation with the Secretary of State, as is the case at other independent UK regulators. While we support the use of a public appointments process for the non-executive and Chair roles on the Board, it should be the Board's responsibility to appoint the Chief Executive which they then hold to account. We believe this is important for all aspects of our remit, but it is absolutely critical for our oversight of government under data protection and freedom of information legislation.

We also note that Convention 108+ states that "The supervisory authorities shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions." The method for appointing members and the adoption of decisions without being subject to external interference are both highlighted as elements that contribute to safeguarding the independence of the supervisory authority. It will be important that the Government consider how its proposals would align with these requirements.

In addition, we believe that both these proposals would result in more significant and frequent government interventions in the ICO's regulatory work than is seen at the other UK digital regulators. It is our view that this does not accord with our role in overseeing compliance by government.

We note the proposals for the ICO to take on the functions of the current Biometrics Commissioner and Surveillance Camera Commissioner roles. It is for Government to decide where these functions would best fit. Should this be what Parliament and Government decide, we are open to this expansion of our role, given the synergies

with our existing responsibilities. This is subject to appropriate funding being available. We also recognise that these proposals could potentially improve regulatory certainty for bodies such as the police and help to simplify the overall regulatory landscape.

Continuing to develop the proposals

We recognise that these proposals are still in development. We look forward to seeing more detail, particularly on those areas where the policy proposals are more high level.

As the work develops, it will be important to understand how the various proposals fit together as a package and that the links between the different proposals are well thought through. Key issues, such as the re-use and re-purposing of data and the approach to accountability, would benefit from analysis on what the collective impact would be on the types and volumes of personal data being processed, or how this would be protected and made transparent.

It is important that Government conducts robust analysis of the costs and benefits for members of the public, businesses, public bodies and the ICO, building on the published impact assessment. This analysis should be based on the impact of the proposals as a whole. As the Government develops the proposals it should also consider any other planned legislation likely to affect the wider data protection framework or the ICO's role and remit. It is also important that the ICO has the resources it needs to deliver against any new legislative framework. We look forward to seeing more detail on the impact on people's data protection rights and on the ICO as the Government's impact assessment and analysis is further developed.

Chapter one – Reducing barriers to responsible innovation

1.1 Research purposes

1. Processing of personal data often plays a central role in research which, when conducted with appropriate safeguards, can result in significant public benefit. The current data protection framework provides a flexible regime for scientific research, including a broad approach to the interpretation of "scientific research". We agree, however, that the existing law can be confusing and there are areas where greater clarity may help support responsible research.

2. We are generally supportive of Government proposals in this area. However, we also encourage the Government to consider and consult on whether any proposed legislative changes would make participation in cross-border research more difficult with international research institutions. We are aware the research sector has identified that varying research provisions internationally have caused confusion. This has led to a reluctance by research institutions to share data for secondary research. The importance of global research has grown significantly so it is important that legislative reform also enables international inter-operability.

3. We have set out our views on the specific proposals below:

    - **Proposal to consolidate and bring together research-specific provisions (paragraph 40)**. We agree that the research provisions are difficult to navigate because they are spread across the UK GDPR and the DPA 2018. We welcome Government proposals to consolidate and bring together the research-specific provisions. We stand ready to support Government in further engaging with the research sector to understand what more could be done in this area.

    - **Incorporate a clearer definition of "scientific research" into legislation (paragraph 42)**. We agree that creating a statutory definition of "scientific research" in the operative text of the UK GDPR could provide greater certainty. We also agree that the definition provided in Recital 159, which advises a broad approach to interpretation of scientific research purposes, would provide a suitable basis for a statutory definition. It is important that any definition of scientific research does not go beyond what people

would reasonably expect to be covered by that term. It also needs to be sufficiently flexible to capture any changes in the nature of, and approach to, research in the future. Any proposal for a broader definition than Recital 159 would need careful consideration of the risks and benefits. This includes how it would impact on wider proposed changes to the research provisions.

- **Determining the best lawful ground to apply to the use of personal data for research purposes (paragraph 44)**. The Government is seeking further evidence on the extent of the challenge faced by researchers in determining what lawful ground should be used for processing personal data. It is considering two proposals:
    - clarifying in legislation how university research projects can rely on the lawful ground of tasks in the public interest; and
    - creating a new, separate lawful ground for research, subject to suitable safeguards.

  While universities can generally rely on public task as a lawful ground for processing personal data for research purposes, we agree that clarifying this in legislation may help address uncertainty. We also agree that a new, separate lawful ground for scientific research could provide a simpler framework and greater certainty for researchers. We would support Government in exploring this option further and would be interested in hearing the views of stakeholders on this issue. It is important that any new lawful ground for research comes with appropriate protections.

- **Clarifying in legislation that people should be allowed to give their consent to broader areas of scientific research when it is not possible to fully identify the purpose of personal data processing at the time of data collection (paragraph 48) and stating explicitly that the further use of data for research purposes is both (i) always compatible with the original purpose and (ii) lawful under Article 6(1) of the UK GDPR (paragraph 48).** Further processing of personal data for scientific research is an important area where organisations would welcome further clarity. We support efforts to provide greater legal certainty on the re-purposing of personal data for research purposes.

  There are already some relevant provisions in the Recitals to the legislation. Normally, scientific research projects can only include

personal data on the basis of consent if they have a well-described purpose. But Recital 33 allows this to be described at a more general level where the purpose cannot be specified at the outset. When data is originally collected for non-research purposes, Recital 50 allows that further processing for research purposes should be considered to be both compatible and lawful. However, when personal data has originally been collected under the lawful ground of consent, it is important that consent is both informed and meaningful. We therefore do not consider that Recital 50 allows for the original consent to be 'extended' to cover new processing for research purposes. This is because it would be beyond what people expected when they originally consented. Rather, new consent to this processing would have to be obtained.

However, these provisions are complex to navigate. We consider that the challenges Government seeks to address through these proposals might be resolved to some extent by the addition of a new lawful ground for processing personal data for scientific research purposes. This would also have the benefit of being easy to understand and use. In any case, we encourage the Government to explore with the research sector and other stakeholders whether these proposals would bring benefits. As well as to consider the potential risks and what additional safeguards would be required to mitigate these.

- **Replicating the Article 14(5)(b) exemption in Article 13, limited only to controllers processing personal data for research purposes (paragraph 50).** This exemption currently allows controllers who have personal data they intend to use for research, but who have not collected that data from people themselves, not to have to provide additional information to those people if it would require a disproportionate effort to do so.

- We think the proposed replication of this exemption could be helpful for researchers who collected the information directly from people, especially after a long period. This is provided there are sufficient safeguards to prevent risks to people and preserve public trust in the use of personal data for research. These should include limiting this exemption to scientific research. It is also important for continuing public trust and confidence in research that there are safeguards to prevent organisations stretching the definition of scientific research beyond what people would reasonably expect.

We welcome Government efforts to seek views on what additional safeguards should be considered as part of this proposed exemption.

1.2 Further processing

4. The Government has identified three key areas of uncertainty and is consulting on whether there may be benefits to improving clarity and facilitating innovative re-use of data in these areas:

    - When personal data may be re-used for a purpose different from that for which it was collected. Currently personal data must be collected for a specific purpose and not further processed in a manner that is incompatible with those purposes.
    - When personal data may be re-used by a different controller than the original controller who collected the data.
    - When personal data may be re-used and a new lawful ground may be needed.

5. We agree that greater clarity in these areas would be useful. We welcome the Government's recognition that there will be challenges to ensure re-use remains fair and within people's reasonable expectations.

6. As these are fundamental principles it is important to address them fully in order to maintain public confidence. In particular, we consider that when data has been collected under the lawful ground of consent it is important that such consent remains meaningful. Where consent is the lawful ground it is also important that people retain control over whether and how their data is re-used. Any exceptions to this principle should be limited to circumstances of genuine important public interest (as already permitted under the current law). Any reforms should give people confidence that, in the limited circumstances in which their personal data can be re-used in ways that go beyond their consent, the legislative framework provides adequate transparency and properly considers and protects their rights and freedoms. We would like to see more explanation of the proposals and detailed analysis of the collective impact on the types and volumes of personal data being processed. We would also like more detail of how the Government plans to make sure this information is protected and that transparency is ensured.

1.3 Legitimate interests

7. Government is proposing creating a limited, exhaustive list of types of processing for which organisations can use the legitimate interests lawful ground, without applying the balancing test (paragraph 60). This is intended to give organisations more confidence to process personal data without unnecessary recourse to consent.

8. Organisations must have a valid basis in law (lawful ground) to process data. Using the right lawful ground, and applying it properly, ensures organisations can use data responsibly for legitimate purposes whilst also being held accountable for implementing the required safeguards. Most lawful grounds require the processing to be necessary and proportionate. These are cornerstone features not only of the UK's approach to data protection but of data protection frameworks globally. Ensuring the processing is both necessary and proportionate also guards against unjustified interference with peoples' human rights, which could otherwise be challenged under human rights law.

9. The legitimate interest lawful ground is a flexible provision that allows organisations to use data in ways that support responsible innovation, rapidly advancing technologies and evolving business models. To rely on the legitimate interest ground, organisations need to demonstrate that:

    - the processing of the personal data is in pursuit of a legitimate interest (purpose);
    - the processing of the personal data is necessary to achieve that particular purpose (necessity); and
    - the interests, rights and freedoms of people do not override that purpose (the balancing test).

10. This test is established in UK caselaw.

11. Inherent in outcome-focused, flexible and proportionate regulation is the need to interpret how the law applies in individual cases. A contextual, case-by-case assessment balances risks relating to data processing activities with people's rights, and identifies relevant mitigations. This grounds the approach in risk-based organisational accountability. This kind of accountability is key to other proposals in the consultation.

12. Government is concerned that organisations lack clarity and confidence to carry out the balancing test. They suggest this may be leading to an overreliance on using consent as a lawful ground for processing, where this may not be appropriate. We recognise and share this concern,

particularly as high volumes of consent requests can lower protections for people. This is because, when agreeing to their data being processed, they give little consideration to the implications because of 'consent fatigue'. We understand that applying the legitimate interest ground, and particularly conducting a balancing test, may feel daunting for some organisations. Especially smaller ones less used to thinking about the implications of how data is used and processed. We are therefore supportive, in principle, of measures that could make establishing the lawfulness of processing easier.

13. Government is proposing to resolve this by producing an exhaustive list of types of data processing where organisations would not be required to assess the balance. The balancing test would not be needed because the Government would include only examples where the impact on people's rights would not outweigh the interests of the organisation seeking to use their data (paragraph 60).

14. In fact, this proposal does not remove the need to undertake an assessment. Rather, it moves the responsibility for doing the relevant thinking from the business to Government. Government would need to be confident that the types of processing they include when drawing up such a list do not have a disproportionate impact on people's rights. Parliament would need to be similarly assured when passing any such list into law.

15. We can see that there could be benefits to this for some organisations. This is because Government is likely to have a greater understanding of the impact of data collection and processing than some businesses. In particular, small organisations that process personal data in limited ways. However, in order for Government to have the required confidence, any such list would need very clear parameters. It would need to set out the nature, context and detail of the processing, given that this is all relevant to assessing where the balance lies. We are concerned that as currently set out in the consultation, the types of processing are too broad to provide the necessary certainty. We are pleased that the consultation recognises the importance of putting these parameters in place and seeks stakeholder views on how this can be achieved. We will be looking for Government to set out the nature of the specific types of processing in more detail and how it has assured itself that those included in the list would not have a disproportionate impact on people.

16. We would also welcome more detail on how this proposal will interact with the exercise of people's rights. For example, the right to object, where a

data controller can only refuse a request if they have a compelling reason that overrides people's interests, rights and freedoms.

1.4 AI and machine learning

17. The consultation is clear that development of AI and machine learning applications is contingent on data, and places specific demands on its collections, curation and use (paragraph 64). It also flags the publication of the Government's National AI Strategy[11], which sets out the Government's intention to review the regulatory governance of AI in a forthcoming White Paper. We agree with Government that AI is built on data. We expect the ICO will maintain its role in overseeing how personal data is processed by AI and other automated decision-making systems, helping ensure this is done responsibly and in ways that build trust.

Fairness in an AI context

18. When people's data is processed, including when it is used to make decisions that affect their lives, both the process and the outcomes should be fair.

19. Fairness has long been a central component of both UK and international data protection legislation, including under the DPA 1998, Convention 108 and 108+ and now under UK GDPR. Article 5(1)(a) of UK GDPR requires that personal data must be processed lawfully, fairly, and in a transparent manner. The concept of fairness as requiring consideration of the balance of interests between people and those seeking to use their data, including the data controller, is reflected across the legislation. It applies to all forms of data processing, not simply to AI, and is central to international data protection frameworks. However, fairness is particularly important in the context of AI, which allows for greater volume and complexity of data processing.

20. We welcome the recognition in the consultation of the importance of fairness in data protection. We acknowledge there is considerable complexity in this area. We welcome the Government's intention to explore these issues further through the development of the National AI Strategy (paragraph 64). However, we would be deeply concerned if any future proposals or developments in this area resulted in the removal of the centrality of fairness in how people's data is used. As this work evolves data protection legislation should continue to ensure that when people's data is processed they are treated fairly. The ICO should

[11] National AI Strategy - GOV.UK (www.gov.uk)

continue to play a role in upholding that, working collaboratively with others, including other regulators, where appropriate.

21. In the consultation, the Government asks whether respondents agree that "The development of a substantive concept of outcome fairness in the data protection regime, that is independent of or supplementary to the operation of other legislation regulating areas within the ambit of fairness, poses risks?", particularly with reference to regulatory confusion for organisations, (Q1.5.4). In response, we would argue that the concept of fairness in data protection does not and should not operate in a vacuum. We recognise the role of other regulators in defining what fairness means in their specific context. We recommend that the ICO is charged with cooperating with these authorities, building on successful models such as the Digital Regulation Cooperation Forum. Cooperating in this way would also help support a level playing field for businesses committed to adhering to fairness requirements. It would ensure they are not competitively disadvantaged if others choose not to comply.

22. Fairness in data protection is not only about transparency – providing people with information so that they understand how their data is being processed. As the consultation notes, while this was a historic focus, fairness now also ensures that the way in which people's data is processed does not lead to unfair or unjustified impacts on their lives. This is important because simply telling someone what you are doing with their data does not, by itself, make it fair. In AI, fairness is also a crucial part of addressing information and power asymmetry, which can otherwise be a feature of these systems. We would be deeply concerned about any clarification or changes to the data protection regime that removed the centrality of fairness in how people's data is used (paragraph 79), including fair outcomes. Data protection legislation should continue to ensure that when people's data is processed they are treated fairly. The ICO should continue to play a role in upholding that, working collaboratively with others, including other regulators, where appropriate.

Building trustworthy AI systems

23. The consultation sets out the Government's ambition to enable organisations developing and deploying AI tools responsibly to benefit from the freedom to experiment, where it does not cause harm. It asks respondents to consider whether organisations should be able to use personal data more freely. For example, for the purpose of training and testing AI responsibly, in line with the OECD Principles on Artificial Intelligence (paragraph 84). This is in addition to existing initiatives such

as the ICO's Regulatory Sandbox that enable innovators to test and trial ideas under regulatory supervision.

24. The consultation points to a "general uncertainty for those looking to deploy AI related tools, or to use personal data to help train system development, and to understand how that activity fits within the current regulatory environment". It explains that the Government is considering how to develop a safe regulatory space for the responsible development, testing and training of AI (paragraph 82). It also points to existing guidance, including the Central Digital and Data Office's Data Ethics Framework, and the work of the Centre for Data Ethics and Innovation on how to deliver responsible innovation.

25. We agree that there is uncertainty in this area, both among organisations and the public. Guidance is important and we have a range of guidance and information available for organisations and the public. This is in addition to the ICO's internationally recognised regulatory sandbox, which does important work in supporting organisations who are developing cutting edge approaches to data use. This guidance helps people understand how organisations use data and what their rights are. It ensures organisations are able to innovate effectively and responsibly and are building data protection considerations in from the start. We are committed to continuing to provide support in this area.

26. We also agree with the statement in the consultation that any move to allow organisations to use personal data more freely must be accompanied by appropriate safeguards. Sandboxes can bring greatest value when they are used to explore new and uncertain ways of using data. This means that there may also be uncertainty about whether these new approaches might cause harm. Sandboxes with appropriate safeguards, including the involvement of the regulator, can therefore bring greater value. This is because they allow more freedom to experiment, while ensuring people whose data is being used are not put at risk. Appropriate safeguards also build wider public trust and confidence in the system. It is important that Government clearly sets out more detail about how such an approach would work and what safeguards would be in place. This includes what the role would be of the ICO as the regulator in helping to provide the proposed regulatory safe space.

27. The consultation also emphasises the importance of monitoring, detecting and correcting bias in AI systems (paragraph 85). It notes that personal data may need to be used for this purpose. It proposes including processing personal data for this purpose in the list of processing that

constitutes a "legitimate interest" in Article 6(1)(f) for which the balancing test is not required (set out above in section 1.3). We agree that relying on legitimate interests is a logical approach for organisations to adopt. However, we would like to see more detailed analysis of the thinking Government has done as part of its assessment that the legitimate interests of the organisation undertaking this kind of processing would always outweigh the potential risks to people's rights and freedoms. In particular, due to the potential sensitivity of some of the personal data likely to be involved. We also note that public authorities may be able to use the lawful ground of public task, if using AI to carry out their functions.

28. The consultation also has proposals for when bias monitoring, detection or correction can only be undertaken with the use of sensitive personal data. In this situation, they will either:

    - make it clear that the existing derogation in Paragraph 8 of Schedule 1 to the DPA 2018 can be used for this type of processing. This derogation covers data processing for the purposes of 'equality of opportunity or treatment'; or

    - create a new condition within Schedule 1 that specifically addresses the processing of sensitive personal data as necessary for AI system bias monitoring, detection and correction.

29. Our preference is the creation of a new condition within Schedule 1. This is because "equality of treatment" is not designed for this purpose and does not encompass all the types of special category data that may be processed. A separate condition allows for more tailoring to the purpose and inclusion of appropriate safeguards (ie beyond just having an appropriate policy document (APD)).[12]

30. More broadly, when considering how best to build trustworthy AI systems, the data protection principles of transparency, fairness and accountability are central. We stress the importance of effective risk assessment and mitigation as part of the approach to accountability. Data protection impact assessments (DPIAs) can play an important role in facilitating this. We also welcome the further work that is underway as part of the National AI Strategy and Centre for Data Ethics and Innovation's AI Assurance workstream. This is assessing the need for broader algorithmic

[12] This approach would also align with the likely approach at EU level in the Artificial Intelligence Act, which Government may wish to consider as part of an assessment of the wider costs and benefits of alignment with other international approaches.

impact assessments, which could also play an important role in ensuring transparency and accountability.

Automated decision-making and data rights

31. We are pleased to see the inclusion in the consultation of a broader discussion on how effectively Article 22 is currently working (paragraph 97). Article 22 does not apply to all automated decision-making. It is intended to protect people when an organisation is carrying out decision-making solely by automated means, without any human involvement, where that decision-making has legal or similarly significant effects on them. These decisions are often made using AI. Article 22 requires organisations to:

    - give people information about the processing;
    - introduce simple ways for them to request human intervention or challenge a decision; and
    - carry out regular checks to make sure their systems are working as intended.

32. Feedback we have received from stakeholders through our work on AI indicates this is a complex area where more engagement would be of benefit. We also recognise that the use of AI is increasingly making automated decision-making mainstream. We need to ensure that Article 22 continues to work effectively in this context. We therefore welcome the consultation's focus on how to provide more clarity and guidance. However, we do not agree with the Taskforce on Innovation, Growth and Regulatory Reform that the right to human review should be removed. Having the right to human review of decisions that can fundamentally affect our lives has been part of data protection law for many years, including prior to the GDPR. It is important, not just for ensuring that those decisions are fair and based on accurate information, but also for promoting public trust and privacy respectful innovation. Removing this right could lead to a perception that decisions are made purely by unaccountable algorithms. This could undermine public support for the use and deployment of AI, even where it delivers substantial economic and social benefits.

33. A more effective approach would be to consider how the current approach to transparency could be strengthened. This would help ensure human review is meaningful and that human reviewers have access to the information and skills they need to scrutinise the ways in which decisions are made. This should be based on detailed analysis and evidence of how

AI enabled decision-making is currently being deployed, and how this is likely to develop in the future. More meaningful transparency, rooted in real-world deployment, would help avoid the risk that any human reviewer simply accepts the AI generated decision without effective scrutiny or challenge.

34. We also encourage Government to consider extending the right in Article 22 to also cover partly automated decisions. We think this would better protect people, given the increase in decision-making where there is a human involved but the decision is still significantly shaped by AI or other automated systems. We acknowledge that more guidance would have to be provided on how human reviews can be provided at scale as AI usage grows. We think this is likely to require a risk-based approach to the depth and nature of human reviews to make it feasible. We are happy to engage further with Government on these issues and support wider engagement with interested stakeholders.

Public trust in the use of data-driven systems

35. We welcome the discussion in the consultation on the use of inferred data, particularly in the context of profiling and AI (paragraphs 104 to 112). Where inferences relate to identifiable people, they will be personal data, and therefore within the scope of data protection law. However, this is an important and challenging area where greater stakeholder input and debate is welcome. We will continue to provide organisations with guidance and support in this area. We welcome the Government's intention to explore this further through the development of the National AI Strategy.

1.5 Data minimisation and anonymisation

Clarifying the circumstances in which data will be regarded as anonymous

36. We welcome the Government's proposal to provide further clarity and certainty about the test organisations must apply when deciding whether information can be considered anonymous and therefore outside the scope of data protection requirements. Two options are under consideration. The first would place text from recital 26 of the UK GDPR on to the face of the legislation (paragraph 121(a)). This states that when determining whether a person is identifiable, account should be taken of "all the means reasonably likely to be used" to re-identify the person. This includes all objective factors, like cost and time, in light of available technology at the time of processing and technological developments.

37. The second option would be to base the test on explanatory text that accompanies the Council of Europe's modernised convention 108+ (paragraph 121(b)). This states that data will be deemed anonymous when it is impossible to re-identify people. Or, if such re-identification would require unreasonable time, effort or resources, based on a case-by-case assessment of factors including cost, the benefits of identification, type of data controller and available technology. Again, noting that this may evolve over time.

38. In our view either option is feasible and would offer additional clarity and support to organisations. Our preference is the first option, translating the text of recital 26 of the UK GDPR. This is on the basis that it would be simple and pragmatic given that this is linked to existing legislation and, in fact, has been constant for more than twenty years. This same approach was included in the directive that underpinned the DPA 1998 and also adopted in the ICO's anonymisation code. It would therefore be familiar to many organisations and is addressed in existing caselaw. Incorporating this text into the DPA would ensure that it applies across all aspects of the regime. It may also be beneficial to clarify in legislation that ICO guidance will be a further aid to following the test. It is also worth noting that the text in recital 26 is the same as in recital 21 of the law enforcement directive which is the basis for the law enforcement provisions in part 3 of the DPA. This further promotes simplicity and consistency.

Clarifying that the test for anonymisation is a relative one

39. The Government is also proposing to clarify that the question of whether data is anonymous is relative to the means available to the data controller to re-identify it (paragraph 123). This would not change the existing position that the test must apply differently over time, taking into account technical developments. Therefore, ongoing due diligence would still be expected. It would also maintain the position that whether data is anonymous or not can be different depending on whose hands it is in. For example, depending on the skills, capabilities and technology available to the person with access to the data. A relative test involves assessing what is "reasonably likely" relative to the specific circumstances, rather than a purely hypothetical chance of identifiability.

40. We support this proposal and agree that it may build confidence amongst organisations to anonymise information and use it more innovatively within their own activities or when sharing with others who adhere to similar standards on anonymisation. It would align well with the guidance

and support materials that the ICO is currently developing on anonymisation.

1.6 Innovative data sharing solutions

Data intermediaries

41. The Government has invited views on its work to support innovative data sharing solutions, while maintaining protections for people. It describes how data intermediaries can help support delivery and manage risk for some of the data protection proposals set out in the consultation. It envisages intermediaries helping to ensure that data is aggregated, processed or shared according to the law, as well as according to parameters or safeguards defined by data providers and data users.

42. We support the Government's intention to provide organisations with additional support in understanding risk and ensuring appropriate protections are applied (paragraphs 135 to 137). Approaches to new, innovative, and appropriate forms of data sharing are to be welcomed. In particular, where they enhance people's rights and have the potential to address power imbalances between those holding large scale data sets and those seeking to use them. For example, through data trusts. However, we believe stakeholders will want to understand more about how these arrangements ensure accountability. This includes ensuring:

    - clarity about who is responsible for ensuring appropriate protections;
    - the principles of data limitation and minimisation principles have been applied;
    - people are able to exercise their rights;
    - we are able to exercise our supervisory duties; and
    - clarity about the nature of the controller and processor relationship.

Chapter two – Reducing burdens on businesses and delivering better outcomes for people

2.1 Reform of the accountability framework

43. Accountability is a central element of a high standards data protection regime, both in the UK and internationally. Supporting organisations to be accountable is a priority for the ICO. This is demonstrated by the importance we have placed on developing our widely consulted on accountability framework[13]. Helping organisations build effective accountability practices into their culture is also important for sustaining high data protection standards in the longer term.

44. We welcome the Government's commitment to enhance and strengthen accountability as a fundamental principle of data protection. We also support its intention to explore whether a greater focus on outcomes in this area could help achieve higher standards. We agree that the current model may create burdens, particularly for smaller organisations undertaking low risk processing. Simplifying and clarifying the law could make it easier for organisations to adopt a flexible, risk-based approach to protecting people's data.

45. The Government proposes a new approach to accountability based on the introduction of risk-based privacy management programmes (PMPs) (paragraph 145). As an alternative, the Government has also suggested a small number of targeted changes to the existing UK GDPR requirements, if it decides not to pursue the PMP approach. We are open to different approaches of ensuring accountability, including those focused more on achieving positive outcomes than on detailed prescription in the law. However, to ensure positive outcomes it is important that any approach is risk-based. This means that those organisations whose processing carries the highest risk to people should also have the more robust approaches to accountability. We look forward to hearing people's views and working with Government to develop its preferred option.

46. It is crucial that any approach to accountability is enforceable. We welcome the proposal in the consultation that organisations should make available, on request, their privacy management programme and accompanying documentation to enable the ICO to continue to enforce the legislation effectively. We also welcome the proposed requirement for the ICO to take into account the quality and effectiveness of a privacy management programme when taking enforcement action.

[13] Accountability Framework | ICO

47. The approach to accountability must include a focus on organisations being accountable for their practices and demonstrating their accountability in a proportionate way, even when detailed requirements are not set out in law. This is important for transparency and public trust and ensuring effective regulatory action can be taken where necessary. A strong approach to accountability is also a central element of an effective international transfers regime. In this case the onus is on the exporter to assess the risk and be accountable for managing that appropriately. Accountability is therefore also essential for global data flows and UK trade and is also a key component of the OECD guidelines.

48. The Government proposes to **remove or amend the requirement to appoint a data protection officer (DPO)** in both approaches. Although it does still include a requirement to appoint a designated individual to oversee data protection compliance. We agree that it is reasonable for many organisations to assess the most appropriate way of assigning responsibility for data protection compliance within their organisations. However, we emphasise the significant skills and experience and professionalism that DPOs can bring. The DPO role under GDPR has also enabled more effective provision of independent advice within organisations and visibility in corporate governance at board level. It is important that those benefits are not lost as a result of any changes. It is also important that Government considers the potential economic impact of removing the requirement for DPOs as part of its overall assessment of the costs and benefits. This is because it is now a well-developed and skilled profession.

49. We also note that the requirement to appoint a dedicated role to ensure importance compliance functions are carried out is a widely used approach across many different sectors. It provides both assurance and expertise. For example, the FCA requires authorised firms and consumer credit firms to appoint an "approved person" to carry out "controlled functions". These include compliance oversight, money laundering reporting functions and senior management functions. The approved person must know and meet the FCA's regulatory requirements and understand how the FCA apply them.

50. Other examples include Schedule 46 of the Finance Act 2009[14] which indicates that, in "qualifying companies", a senior accounting officer must be appointed. Their role is to monitor the accounting arrangements of the company, and to identify any ways in which those arrangements are not appropriate tax accounting arrangements. The UK's Money Laundering

[14] https://www.legislation.gov.uk/ukpga/2009/10/schedule/46

Regulations 2017[15] require all businesses within the regulated financial services sector and some law firms to appoint a Money Laundering Reporting Officer (MLRO). The MLRO provide oversight for their firm's anti-money laundering (AML) systems, and act as a focal point for related inquiries. And employers who have five or more employees must appoint a competent person or people to help them meet health and safety legal duties as set out in Regulation 7 of The Management of Health and Safety at Work Regulations 1999[16]. This competent person should have the skills, knowledge and experience to be able to recognise hazards in the business and help to put sensible controls in place to protect workers and others from harm.

51. We would encourage Government to consider how to retain the value, expertise and assurance that DPOs currently provide. This is particularly important in organisations with the highest levels of data use and consequently the highest potential risk to people. Having a dedicated role with responsibility for ensuring people's data is properly protected is an important safeguard.

52. **Breach reporting.** We support proposals under both approaches to clarify the threshold for reporting data breaches. We know organisations are sometimes unclear on when and whether they should report a personal data breach, and that this can result in over-reporting of low-risk incidents. We have produced guidance[17] on when to report these breaches, including tailored advice for SMEs, but greater clarity in the legislation could be helpful.

53. We note that the Government is considering changing the threshold for personal data breach notification. This would mean that organisations must report a breach to the ICO, unless the risk to people is not material. We are supportive of exploring the most appropriate threshold for data breaches. However, it is important that a comprehensive assessment of risk is used. While some breaches may cause little individual harm, they may cause significant societal harm due to the number or characteristics of people most affected. The Government would need to ensure that such a change to the reporting threshold takes account of this.

54. We note that data breach reports can be a valuable source of insight into the threats facing the wider cyber security landscape. We would want to ensure that any changes made to the threshold did not reduce the ability

[15] Money Laundering Regulations 2017 (ifa.org.uk)
[16] https://www.legislation.gov.uk/uksi/1999/3242/regulation/7/made
[17] 72 hours - how to respond to a personal data breach | ICO

of the ICO and other relevant organisations to assess and address these threats.

55. We also recognise the importance of supporting any changes to the law through revised ICO guidance. Given the potential impact of security breaches on people's lives, infringements of the new reporting requirement should result in the same sanctions as under the current regime.

Accountability based on privacy management programmes

56. Under this proposal, organisations would be required to develop and implement a risk-based "privacy management programme" (PMP) that reflects the volume and sensitivity of the personal data it handles and the types of data processing it carries out.

57. It is important that this less prescriptive approach to accountability is underpinned in law, with a requirement to be accountable and to demonstrate compliance with the law. It is also important there is clarity that PMPs should be in place from the design stage, not just after processing has begun. This is particularly the case for novel or complex processing. This would reduce risks to people and ensure privacy by design can be built in from the start. It is also important to understand in more detail from Government how the PMP proposal would ensure a risk-based approach. This includes how it would ensure that those organisations with the highest volumes, greatest complexity or most privacy intrusive data have the most robust approaches to accountability and risk identification, mitigation and management. This should include when organisations are using novel technologies or approaches, where the risks to people may be less well understood.

58. It is also essential that this proposal is implemented in a way that does not create greater burdens for organisations, including SMEs, than the current legislative framework, or undermine protections for people. We welcome the Government's recognition that many organisations have invested time and resources to establish policies and processes to become UK GDPR-compliant. We support the proposal that organisations would not be required to change many of their current processes if they already operate effectively. But would have the flexibility to do so, if other processes can deliver the same or better outcomes in more meaningful, innovative and efficient ways. However, we think there is still more work for Government to do to set out whether the additional benefits that a PMP approach would bring would outweigh the potential costs involved in making these changes. We also encourage Government to explore whether these benefits could be achieved with more minor changes to the

level of prescription in current accountability requirements, avoiding the potential disruption that could come with more substantial change.

59. We agree with the Government's assessment that some organisations may be better equipped to take advantage of this new flexibility. It says guidance should be available from the ICO. For those organisations that lack the capacity or expertise to design their own accountability practices without support. The ICO is well-placed to help organisations develop the foundations of an effective privacy management programme. Our well-received accountability framework provides a practical tool to support organisations to put in place appropriate, risk-based data protection measures. We have designed it to be flexible in keeping with the scalable nature of accountability and we can update it to reflect changes to the legislative framework.

60. **DPIAs and prior consultation with the Information Commissioner's Office.** The consultation includes a proposal to remove the requirement to conduct a DPIA, replacing it with a more general requirement to identify and minimise data protection risks in a way that best suits the organisation (paragraphs 147 and 159).

61. Our experience shows that DPIAs are a powerful tool which compel organisations to:

    - map the ways in which they are using personal data;
    - identify and understand the risks to people that this creates;
    - explicitly record risks; and
    - take appropriate steps to manage and mitigate them.

62. This can result in changes of approach to the processing and ensure privacy is designed in from the start. They also enable the ICO to intervene to ensure personal data is effectively protected, including using enforcement action, where appropriate. While we agree that there is scope for more flexibility about the form that these assessments take, it is important that this does not result in a reduction in the robustness or quality of those assessments. We would also welcome more detail from Government about how these proposals would enable businesses to assess the risks of harm to people that arise from new or novel processing, particularly where these involve new technology.

63. The consultation also proposes removing the requirement in Article 36 to consult the regulator when a DPIA has identified a high risk to people's rights and freedoms that can't be reduced (paragraph 172). The ICO does not receive large numbers of these requests. This indicates that the provision does not currently represent a significant burden for business.

However, of those we do receive, one in four results in a warning to organisations about their intended processing. It is important to note that this is not a barrier to innovation, as none of these warnings have resulted in the processing being abandoned. Rather, ICO engagement ensured appropriate protections or privacy-respecting approaches were put in place. This approach enables and supports innovation, helping organisations to mitigate risks. Removing this provision would remove an important opportunity for the ICO to offer proactive support to organisations carrying out the most potentially high risk processing.

64. We are also concerned that this reform could undermine a generally positive direction of travel. Organisations are recognising the need to assess risk and want to get things right. Since the prior consultation requirement was introduced, we have received more DPIAs from organisations wanting to engage proactively with the ICO than before it was introduced. One of the valuable elements of the current approach is that organisations need to satisfy themselves that prior consultation is not required. This encourages organisations to consider their data processing in the round by looking at the likely risks of harm to people and how to manage these, even where they conclude that this does not necessitate prior consultation.

65. We agree there is scope to reform the current approach. But rather than remove the requirement we recommend introducing a more agile and flexible threshold for when prior consultation is required. One that is better able to reflect emerging risks and public concerns. Reforming the threshold would also better support organisations to identify the kinds of risks where pre-consultation would be required. Removing the statutory framework for scrutiny of high-risk processing could undermine the high standards of protection for people we know Government is committed to. It could also be seen by many stakeholders as a reduction in transparency.

66. The importance and relevance of DPIAs was highlighted in high profile use cases during the pandemic. They have been an invaluable tool for controllers to plan and implement their approach to protecting personal data. DPIAs have also provided a vital framework for engagement between the ICO and Government or devolved authority about Covid-19 responses. They enabled us to get up to speed with key issues rapidly and, when time permitted, provide strategic advice and assurance that controllers had considered their compliance obligations. Without this tool, it would have been difficult to understand the breadth of data protection issues as quickly and efficiently or to provide the interventions to protect the public in as timely a manner.

67. The use of DPIAs in this context meant we encouraged organisations to consider data protection risks early and adopt a privacy by design approach into their responses and actions from the design stage onwards. Without DPIAs, and their key features (including a systematic description of processing), it would have taken much longer for the ICO and the organisations we worked with to understand the risks to and impact on people's rights as we all sought to respond to the pandemic. It may also have resulted in less effective responses. For instance, if people's personal data had not been properly protected, resulting in them not trusting organisations enough to share their data.

68. Examples that illustrate the positive impact DPIAs had during the pandemic include:

    - ICO's work with Public Health England (PHE), the Department for Health and Social Care (DHSC), the Northern Ireland Public Health Agency and Department of Health and the Scottish Government on track and trace, including the manual tracing systems and contact tracing apps.
    - Work with the DHSC on the DPIA for their bulk risk stratification tool (QCovid model). This processes personal data to estimate people's risk of being admitted to hospital and their mortality risk should they contract the virus. It includes a functionality that can stratify the population to identify those most at risk but who were not otherwise identified as Clinically Extremely Vulnerable.
    - Work with private and public sector bodies on temperature testing in airports.
    - Work with businesses on private testing regimes for staff.

69. In all these examples, we worked closely with organisations to build in key data protection considerations from the outset. This ensured fast delivery of crucial interventions while also protecting people's data and privacy and securing public trust in the process.

70. **Record keeping.** The Government proposes to remove record keeping requirements under Article 30 UK GDPR. Organisations would still be required to understand what personal data they process, and where and how it is processed, but with no prescriptive requirements for what they would need to include in the record. Keeping good records is a key element of good privacy management and high standards of privacy. It also supports organisations to deal effectively and efficiently with subject access requests. Also, in some cases with requests made under the Freedom of Information Act and Environmental Information Regulations.

There is scope, however, to explore reducing prescriptive record keeping requirements, particularly for smaller organisations undertaking low risk processing.

71. The Government acknowledges that removing the records of processing requirements under Article 30 could hinder effective enforcement and offer less regulatory protection to people. To address this, they would encourage the ICO to develop straightforward guidance for organisations to help them meet the new requirements. We are in a good position to do so, building on the guidance in our accountability framework, which we continue to review and develop.

72. **Voluntary undertakings process.** The Government is considering introducing a new "voluntary undertakings process" (similar to Singapore's "Active Enforcement" regime) (paragraph 181). It proposes that if an organisation can demonstrate it has embraced a proactive approach to accountability, it may provide the ICO with a remedial action plan upon discovering an infringement. The ICO may authorise this plan without taking any further action, provided it meets certain criteria.

73. It is important the proposal to allow an organisation to enter voluntary undertakings with the ICO in the case of serious infringements does not reduce our ability to use our regulatory discretion to act based on all the circumstances. This should be the case even where an effective management plan is in place.

74. If this proposal is to be effective, the ICO needs to retain discretion to choose whether to accept a remedial action plan as sufficient. The ICO also needs to retain inspection powers to ensure compliance has been achieved. This is to ensure we are able to act further down the line if we are not satisfied with the implementation of any such plan, or where deficiencies in a plan are identified during an investigation into a serious breach. There should be a clear formal process for reporting any infringements, so that we are clear where there has been an issue, even where voluntary undertakings are accepted.

Stand-alone reforms if the Government decides not to pursue PMP approach

75. The Government suggests that certain elements of the accountability proposal could be implemented as stand-alone reforms, if it decides not to pursue the PMP approach. This alternative approach is based largely on the current requirements but with targeted changes in specific areas to reduce the administrative burden placed on organisations. These include:

- **Record keeping.** The proposal under the PMP approach to remove record keeping requirements would not be implemented in full and certain elements may be amended.
- **Breach reporting.** The Government proposes the same reforms to the breach reporting thresholds for both approaches.
- **DPOs.** The Government is considering changing the threshold above which smaller public authorities are required to appoint a DPO. As noted above, DPOs can bring significant experience and professionalism to data protection compliance. We know some smaller public authorities increase efficiency by using a shared DPO to provide input across multiple authorities. However, we are aware that despite this the current requirements for smaller public authorities not carrying out high intensity or high risk data processing can be burdensome. They are also not in line with the requirements for similarly sized private sector organisations. We therefore support the proposal to reforming this requirement proportionately according to the risks of the processing likely to be undertaken by such authorities.

2.2 Subject access requests

76. The Government is proposing several changes to the requirements for processing subject access requests (SARs). These give people the right to ask for the personal information held about them; information that can often be used to make significant decisions about their lives. Concerns fall into two broad categories. The first is whether organisations have the capacity to process requests, particularly where volumes are high (ie bulk requests) and where smaller organisations have limited resources. The second is the threshold for responding to requests. Government has concerns that SARs can be used where there is no intention to exercise data protection rights but instead to circumvent other disclosure regimes, such as the Civil Procedure Rules[18] or simply to cause disruption. Government is concerned that existing grounds for refusing to comply with a SAR, where a request is "manifestly unfounded or excessive", impose a high bar for refusal. Also that it can be difficult to determine when it is appropriate to enquire about the purpose of a request or to consider the context and history.

77. To address the issues outlined above, the Government's proposals include reintroducing a nominal fee for making a SAR. This existed under the DPA

[18] Part 31 of the Civil Procedure Rules govern the rules of disclosure and inspection of document in Civil Court proceedings.

1998 and also applies under Part 4 of the DPA 2018. It is also looking at the potential to create a cost limit similar to section 12 of the FOIA. It proposes replacing existing manifestly unfounded and excessive provisions with an approach similar to section 14 of FOIA. This permits refusal of a request on the basis that it is vexatious, having taken into consideration the context and history of the request and assessment of the burden involved in responding. There is also an open question in the consultation about whether it would be appropriate to introduce a duty on organisations to provide advice and assistance to people. This would be comparable to the duty in section 16 of FOIA (paragraphs 188 and 189).

78. We welcome the Government's recognition of the importance of subject access requests (SARs) as a mechanism for delivering the fundamental and longstanding right of access. We also welcome the commitment to protect SARs as a critical transparency mechanism. In particular, as they often act as a gateway for people seeking to exercise other data protection rights, as well as broader rights. A study by Harris International prepared for the ICO found that 20% of those asked about the importance of their data rights deemed the right of access to be the most important, with 49% ranking this in the top three most important. Overall, the right of access ranked first of the eight options [19].

79. We recognise that some SARs can create a burden for some organisations, particularly in the context of bulk requests. We support the intention to offer further clarity about when requests could be refused as vexatious. However, in an increasingly data-driven world, it is important that reforms do not undermine the right of access, given the role it plays in supporting people to understand what information is held about them and how this impacts decisions that affect them.

80. Organisations benefitting from the personal data they process need to comply with the law and adopt a data protection by design and default approach. This should include automating requests, ensuring information management systems facilitate dealing with SARs, and using tools like dashboards and downloads where possible. This supports the exercise of people's rights and their links to consumer rights. This is also likely to reduce the burden of responding to requests and increase public trust. It is also relevant to note that under the current regulatory framework, controllers can ask people to specify the information or processing activities the request relates to before they provide information. As

[19] ICO Information Rights Strategic Plan: Trust and Confidence pg 36

confirmed in ICO guidance, controllers are not required to respond until that further information is provided[20].

81. The ICO works constructively with data controllers to address some of the practical challenges they may face when managing responses to SARs. For example, we have worked with local authorities to support them in implementing changes to streamline their procedures, combining identity verification measures and requests for clarification of the information sought, to speed up response rates and improve customer service. We have flagged the importance of taking a data protection by design approach when procuring and configuring new IT systems so that they facilitate providing information to people who may exercise their right of access.

82. We recognise the need for proportionality in balancing the impact on organisations. But we are concerned about the lack of consideration of the impact on people and the potential for these changes to reduce people's ability to access their fundamental rights. While there are many useful lessons that can be learnt from FOIA, the issues raised are not the same. For instance, the information that people seek may have a profound impact on their lives. For example, where they seek information from their care record or information about their own health or decisions made about them in the context of benefits, insurance or similar. It is reasonable to suppose that the SARs regime is more likely to be used by people with limited financial means and who may be vulnerable in other ways.

83. It is also relevant to note that where requests made under FOIA are refused, on the basis that they are vexatious or would exceed the cost limit, the requester can bring a complaint to the ICO. Subsequently they can appeal against the outcome of that complaint to the First Tier Information Tribunal free of charge. Under the DPA 2018 people can complain to the ICO and they can also apply for a court order requiring a data controller to comply with a request at their own cost. We support the introduction of a duty to provide advice and assistance similar to the FOIA section 16 duty, to balance the overall impact on people. But we would like to see further detailed consideration about how safeguards will work in practice, including how any rights of appeal may need to be amended and how potential equality issues will be addressed.

[20] What should we consider when responding to a request? | ICO

84. In our view a fuller assessment is needed to understand the implications of introducing a nominal fee, which potentially has a wide-ranging impact on people. This will ensure that any change is not disproportionate.

85. Finally, poor record management or information handling should not be a reason for elevated cost estimates to avoid dealing with requests. This should be made clear to organisations.

2.3 Privacy and Electronic Communications

Confidentiality of terminal equipment, including the use of cookies and similar technologies

86. We recognise that the existing approach to PECR, particularly in the context of cookies and similar technologies, is not effective. It causes burdens for businesses and friction for users, without providing effective transparency or control. ICO research conducted by Harris International in 2021 shows that over half (53%) of people say that "when prompted, they will agree to accept cookies from a website without looking at the details."[21] We welcome this opportunity to improve outcomes for all parties and to resolve the current issues quickly, providing international leadership on these complex issues.

87. We support the proposal to enable organisations to measure the quality and effectiveness of their online services (eg analytics) without the need to obtain prior consent, subject to appropriate safeguards (paragraph 198).

88. We also note the Government's second proposed option. This would permit organisations to store information on, or collect information from, a user's device without their consent for other limited purposes. This includes processing necessary for the legitimate interests of the data controllers, where the impact on people's privacy is likely to be minimal. The examples given include detecting technical faults or enabling use of video or other enhanced functionality on websites. We think there is an opportunity to explore this further, although any changes would need appropriate safeguards. Many of these purposes are already exempt under the strictly necessary category, and are recognised as such in ICO guidance[22]. But we recognise that further clarity on this in legislation could be helpful. However, it would also be helpful to understand how these proposals would work in the context of the wider reforms outlined in this consultation. This is particularly important given the inclusion of

[21] ico-trust-and-confidence-report-290621.pdf
[22] How do we comply with the cookie rules? | ICO

analytics in the list of data processing activities for which no balancing test is required, which could have the impact of removing safeguards.

89. We support the proposal to explore ways in which browser and software application settings can capture user preferences and ensure these are expressed across all services the user accesses (paragraph 204). Introducing these kinds of browser and non-browser-based solutions, and ensuring that organisations respect those preferences, gives people the power to choose the online experience and level of privacy protection that is right for them, and means people can choose to go pop up free. However, making it work would need effective enforcement to ensure organisations did respect those preferences. This would create a level playing field for organisations who wanted to play by the rules. Delivering this proposal would also require international cooperation, and there is an opportunity for UK global leadership on this issue. We would welcome further discussion with Government to ensure the ICO has the enforcement powers we need to make this solution work for people and businesses. We stand by to support Government in any international engagement it seeks to do on this issue.

90. We also recommend that Government consider the pros and cons of legislating against the use of cookie walls, which require users to 'accept' tracking as the price of entrance. This would need careful consideration but would remove the risk that some sites choose to force people to change their preferences in order to access them and would help drive a change in practice.

91. We are happy to work with Government, regulators and others to explore how the proposed changes can be done in a way that stimulates a wider, competitive market. If done well, we believe this could be a measure that:

    - promotes both privacy and competition;
    - supports innovation by building on, and potentially providing legislative underpinning for, market developments such as new or revised web standards;
    - creates additional functionality by software developers (such as browser manufacturers); and
    - supports the general shift towards reducing harms from widespread or disproportionate data dissemination on the web.

92. The consultation also seeks views on the proposal by the Taskforce on Innovation, Growth and Regulatory Reform that data fiduciaries or other

trusted third parties could play a role in managing people's consent preferences. Also, that such a system could potentially put an end to cookie pop-up notices directed at individual users. We are interested in understanding more detail about how this would work in practice. However, we are concerned about the Taskforce's proposal to remove the requirement for prior consent for all types of cookies. This is irrespective of whether people have set their preferences via web browser technologies or through trusted data fiduciaries. Our concern is due to the highly intensive ways in which this data is processed across multiple organisations. We think the proposals to allow users to express their preferences and then have them respected across all sites they access would better manage the balance between delivering a friction-free online experience for people, while also enabling them to have control over their data.

The "soft opt-in" in relation to direct marketing activities

93. The Government is also considering extending the rules around the "soft opt-in" for electronic communications for direct marketing to cover non-commercial organisations. For example, political parties and charities, where they have previously formed a relationship with the person (eg as a result of membership or subscription). Currently organisations are able to send marketing communications to their customers following the sale of goods or services, without seeking additional consent, if they apply to similar goods and service. This is known as the soft opt-in. This only covers electronic communications, not telephone calls, and there has to be a clearly available opt-out. Under current rules this provision does not extend to the communication of aims and ideals through electronic communications. Political communications from parties and elected representatives and campaigning information from charities are not therefore included in the soft opt-in.

94. We are aware that many non-commercial organisations are concerned that their communications with supporters are subject to more restrictive rules than those that govern how commercial organisations are able to communicate with their customers. We therefore see benefits to the proposal to extend the soft opt-in to communication of aims and ideals. However, any extension should include the existing safeguards that apply to use of the soft opt-in. In particular:

    - the organisation relying on the soft opt-in must have collected the details from people themselves, as the soft opt-in is intended for use where there is an existing customer relationship. It should not

be used by organisations that have bought data they are seeking to use for this purpose;

- as set out in the consultation, people must be given a clear, easy chance to opt-out when their details are collected and in every subsequent communication, so they retain control over the information they receive; and
- the marketing or communication is about similar products, services or issues than those for which people originally gave their details.

95. It is also important to explore further whether the extension of the soft opt-in to cover communication about aims and ideals should include fundraising requests. If so, whether additional safeguards would be required. This is particularly important given previous concerns about high volumes of fundraising material causing distress, and in some cases significant harm, to vulnerable people.

Nuisance and fraudulent calls

96. Tackling nuisance calls is a priority area for the ICO where we are already taking proactive action. We want to ensure people, including the most vulnerable, are protected. Where scams and fraud undermine trust in online or distance selling, we want to ensure that the actions of the minority of bad actors do not have a knock-on impact on trust and confidence in the wider digital economy. The ICO's work on nuisance calls divides into two main categories:

- work to address non-compliant marketing by legitimate companies; and
- work to disrupt theft of personal data for the purposes of generating leads for scammers to market unlawful or harmful products and services.

97. We receive around 130,000 complaints and reports about unsolicited communications a year related to nuisance calls, texts and messages. Our general approach is to focus our resources on the most harmful fraud and scam activities that rely on the unlawful acquisition and misuse of personal data. Utilising the full range of our powers, the ICO's strategy is to deliver regulatory action either in isolation or collaboration, with other agencies such as OFCOM, the Pensions Regulator, law enforcement and Trading Standards and through the work of the Stop Scams project.

98. We take complaints and reports from members of the public, trade and other market organisations on the issue of nuisance calls. The intelligence

we receive informs where we target future investigations. We identify organisations that generate significant complaints or repeated issues. We focus regulatory efforts on themes and issues to draw out observations from sectoral or category trends. Our recent work has included actions against:

- pensions cold calling;
- misuse of QR codes in the context of the Covid-19 pandemic;
- marketing of Covid-19 related products; and
- misuse of Test and Trace data for marketing purposes.

99. We have recently finalised reports on the last two of these campaigns, where we issued several fines as well as undertook compliance activity with over a dozen companies.

100. We welcome the range of additional options set out in the consultation (Q2.4.10-Q2.4.15). We think these could have an important impact on reducing the harm created by these calls. We look forward to understanding stakeholder views on the value these could deliver beyond the activity already being conducted, as well as any more that could be done in this area.

101. We also recommend Government consider extending the UK's existing PECR legislation to operate on an extra-territorial basis, like UK GPDR. This would help the ICO to reach beyond the UK's borders to pursue instigators of calls from abroad that target UK citizens.

Bringing PECR's enforcement regime into line with the UK GDPR and Data Protection Act

102. To bring PECR's enforcement regime into line with the UK GDPR and DPA, the Government is proposing to increase fines that the ICO can impose under PECR. This would put them at the same level as those under the UK GDPR and allow the ICO to impose assessment notices on companies suspected of infringements of PECR to enable them to carry out audits of the data controllers' processing activities (paragraph 218). We support these changes, but there would also be benefit in aligning the whole of the PECR enforcement toolkit with that of the DPA 2018, not just these elements. For example, Regulation 5(6) on security audits is out of step with our DPA 2018 audit power and has no in-built right of appeal. Therefore, if we identify a security issue during a PECR security audit and want to rely on an enforcement notice, we must use powers from the DPA 1998, which is different to the DPA 2018 power and is less helpful.

2.4 Use of personal data for the purposes of democratic engagement

Political campaigning and direct marketing rules under PECR

103. The Government is proposing to support democratic engagement and participation by relaxing the rules on electronic communications that apply to political parties, candidates and third-party campaign groups (paragraph 222). These communications are currently treated as direct marketing under PECR. As discussed above, PECR covers all communication of aims and ideals regardless of who is sending them and would therefore continue to apply to campaign communications from other organisations not specified in any changes.

104. Democratic engagement is an essential element of a healthy democracy. We recognise that political parties need to be able to communicate effectively, using the range of modern communications methods available. However, it is also important this communication is done in ways that foster public trust in how our data is being used. Any approach that undermines that trust could have unintended negative consequences for wider public attitudes towards our democratic processes.

105. The consultation does not go into detail about which elements of these rules would be relaxed. If the requirements under PECR were removed completely for these communications, this would mean that:

- live calls could be made without checking the telephone preference service register (the register of those who have opted out of marketing calls) or previous objections;
- automated calls could be made without consent; and
- electronic mail could be sent without consent.

106. It is important to note that political parties can already communicate more generally by electronic means with those who have consented, where this is necessary under the current rules in PECR, and it is fair and lawful to do so under the UK GDPR. In addition, live campaigning calls, where the call is made by a person rather than automated, do not currently require consent, except for people registered with the Telephone Preference Service. This is set out in Regulation 21 of PECR. Political parties, elected representatives, and those groups who are registered with the electoral commission are also able to access the electoral register of names and addresses, which they can use to communicate with people through traditional mail.

107. Any further relaxation would need careful consideration to ensure the potential wider societal benefits were not outweighed by any negative impacts on people. It is important to consider the following factors as part of any assessment of the costs and benefits:

    - Who any changes would apply to. The consultation references "political parties and other political entities, such as candidates and third-party campaign groups registered with the Electoral Commission". Clarity on exactly who is in scope is important and the broader this is, the greater the potential volume of unsolicited information people are likely to receive. While there is benefit to people being informed, frequent or high volumes of information or both could be perceived as intrusive.

    - The types of communications to which any changes would apply. This will also have a significant effect on the impact on people. For example, changes that were restricted to communications about an upcoming election, within the formal campaigning period, would have a different, and potentially less intrusive impact on people than an approach which relaxed requirements on all types of communications at any time.

    - Whether fundraising communication is included. If requests for financial support were included this could be perceived as intrusive, and could have a negative impact, particularly for more vulnerable people. This could also be seen as an opportunity by those perpetuating scam calls and emails. We know this is already an area of concern for Government and careful consideration would need to be given to ensure the proposals did not inadvertently increase the volume of this activity.

    - The potential impact on the market for personal data. It would be important to consider where political parties and others would be likely to obtain the personal data needed. Also, that this did not inadvertently encourage a market in personal data that was not transparent, or that undermined trust or encouraged poor practice. More generally, it is important that any processing of personal data for these purposes is compatible with UK data protection requirements. This includes those of fairness, transparency and accountability, not just with PECR. Also, that people's data protection rights are retained.

108. We know that this is an area that people care about. Ensuring a healthy democracy is important to us all. However, people also value their privacy. The ICO already receives some concerns relating to

communications from political parties. From January 2018 to June 2020 we dealt with over 600 cases on political parties' use of personal data. While these are not all linked to marketing, in some cases the concerns have arisen because of a direct communication between the party and an individual. Whilst not all of these cases represent upheld complaints, we think this is indicative of an area where a wider public debate would be of benefit. For instance, through direct research with the public to ensure that any changes enjoy wide public support, and appropriate safeguards are put in place. Furthermore, if any changes in this area are taken forward then it is vital that people are given all of their existing rights. This includes those which allow them to object to their data being processed.

109. The Government also proposes that if these rules are not changed, then it is minded to pursue its proposed reforms on the soft opt-in. This would allow political parties to communicate more easily with those who had previously shown an interest. As discussed above, we can see benefits to the proposals on the soft opt-in, subject to the retention of appropriate safeguards. This may result in a more proportionate change. This would depend on the results of the further evidence gathering and assessment that should accompany any such changes to the rules around direct marketing of political communications.

Lawful grounds for processing personal data under the UK GDPR and DPA 2018

110. The Government is also asking about the extent to which the lawful grounds under Article 6 of the UK GDPR impede the use of personal data for the purposes of democratic engagement (paragraph 226). Currently, section 8 of the DPA 2018 sets out that democratic engagement is a public task. To support the use of the public task lawful ground for processing of personal data, there needs to also be a corresponding obligation laid down by law linked to this processing. For the processing of personal data sourced from the electoral register, most campaigners are able to rely upon electoral law. For processing other data under public task, other laws would need to be relied on, which we understand is challenging.

111. Depending on the circumstances, political parties and campaigners can use other lawful grounds. In particular, the consent and legitimate interests lawful grounds, as long as they can demonstrate the processing is necessary and that their interests are not outweighed by any impact on the rights and freedoms of the people whose data they are processing. We therefore think there is already flexibility for political parties and

campaigners in this area. Although, we are interested in hearing from stakeholders where they think further clarity or flexibility would be of value.

112. The Government is also asking for evidence on the use of the conditions for processing in paragraph 22 Schedule 1 of the DPA 2018 (paragraphs 227-228). These set out the conditions under which political parties are able to process data on political opinions without consent. The rules in this area are important because data about our political views and activity is sensitive. There can therefore be negative consequences for people if this is used or shared inappropriately. This is part of a wider set of data which is known as special category data. These are set out in Article 9 of the UK GDPR, along with a set of rules around how this data can be used to protect people.

113. The Government is seeking views on how well these conditions are working. We are interested in hearing stakeholder views on this issue. However, we would be concerned if there was any proposal for an expansion of the kinds of special category data political parties are able to process without consent. For example, if it was to include ethnicity or other data, either factual or inferred. Furthermore, currently only registered political parties can rely on these conditions. It is important to understand if the Government may also consider extending these further to allow candidates and third party campaigners to do so. If any such expansions are considered, it is important that the rationale for why this is required is clearly set out and that there is a wide public debate on the risks and benefits.

Chapter three – Boosting trade and reducing barriers to data flows

114. The UK can now set its own data protection policy. This includes the UK's own approach to importing and exporting data, known as international transfers. It also includes its assessment of the data protection laws of other countries and jurisdictions, to determine if they would uphold or undermine the level of protection for people's data in the UK. This is known as making an adequacy assessment and is set out in data protection law in UK GDPR.

115. The consultation considers how the UK's approach to adequacy regulations may evolve. The consultation also considers the approach to alternative international transfer mechanisms (AITMs). These are tools that implement additional safeguards to protect people's data when it is transferred to jurisdictions not covered by UK adequacy regulations.

116. We welcome the discussion of possible approaches to supporting organisations to continue to import and export personal data easily, whilst maintaining the high standards that will protect people. The UK is well regarded around the world for its track record of high standards of data protection and many of these are now being adopted globally. This applies both to the standards we set domestically and those we set for exporting data from the UK to other countries, where people in the UK expect that those standards will be maintained.

117. UK businesses also rely on the ability to import and export data in a fast-moving global digital economy. For this reason, the certainty that is provided by the EU's positive adequacy decision on the UK's laws has been welcomed by businesses of all sizes in the UK. This decision allows UK firms to continue to import and export data to the EU without further safeguards needing to be put in place. For exporting personal data to other territories, organisations expect to be able to employ risk-based and practical ways to transfer personal data across the world and know how to achieve compliance with our standards.

3.1 Adequacy

A risk-based approach to adequacy regulations

118. The Government's consultation sets out several proposals on how it plans to evolve adequacy regulations under UK GDPR. The Government's ambition is for the UK to be a leader in digital trade and the world's most attractive data marketplace. As part of this, it plans to increase the number of countries who are covered by UK adequacy regulations to

facilitate data flows and trade across borders. To do this, it proposes to take a risk-based approach to adequacy assessments. This would take into account the likelihood and severity of risks to data protection rights.

119. It is the responsibility of the UK Government to assess whether the data protection laws of other countries and jurisdictions provide adequate protection for UK citizens. However, the ICO also has a role. We are consulted by the Government and provide advice and expert input into its decision. Further details on our role are set out in a memorandum of understanding between the ICO and DCMS[23].

120. We welcome the Government's ambition to increase flows of data safely across jurisdictions, and the proposal to approach adequacy assessments with a focus on risk-based decision-making and outcomes. It is important that the approach continues to ensure our existing high standards are maintained. We are pleased to see that the consultation sets out that assessments would take into account, amongst other things:

- the rule of law;
- respect for human rights and fundamental freedoms; and
- the existence and effective functioning of a regulator.

121. While we recognise that these proposals are still in development more detail is needed for respondents to fully understand how a risk-based approach would work in practice. It would also be helpful to understand more detail about the proposals for future adequacy decisions to "take into account the different legal and cultural traditions which inform how other countries achieve high standards of data protection". We look forward to seeing more detail about how these changes would work in practice.

122. Stakeholders, particularly UK businesses, have also consistently stressed to the ICO how important it is for them to secure and retain the UK's adequacy status with the EU. Therefore, any reform of the process to assess and grant adequacy to other countries and jurisdictions should take into account the importance to UK business of retaining our EU adequacy status.

123. Assuring a robust adequacy assessment process is also important for maintaining our position as a trusted jurisdiction for data from many other countries. Data transferred to the UK can then be transferred on to other countries we have assessed as adequate. Ensuring that our approach to maintaining appropriately high standards of data protection is

[23] MoU between the ICO and DCMS on the role of the ICO in new UK adequacy regulations: uk-adequacy-assessments-ico-dcms-memorandum-of-understanding.pdf

respected internationally is therefore crucial for us in order to retain our role as a hub for international data flows.

Creating a scalable, flexible adequacy regime

124. The Government is proposing to extend its ability to make adequacy assessments to include groups of countries, regions and multilateral frameworks (paragraph 248). As above, we look forward to seeing more details or examples of how these proposals would work in practice. Clearly there could be efficiencies to be gained from assessing the laws of a group of countries. For example, where a number of countries are all subject to the same multinational jurisdiction. However, it would be helpful to have more detail about how the Government proposes to deploy this approach to fully understand the risks and benefits involved.

125. The Government also proposes removing the need for periodic review of adequacy decisions, which currently must take place every four years (paragraph 250). This would be replaced with ongoing monitoring of countries that have received adequate status. We can see that this could allow Government to focus its resources on those areas where there is an increase in risk or significant change in circumstances, potentially making the process more flexible and efficient. However, we would be concerned if the proposed approach resulted in a lowering of the Government's ability to detect and act on changes that might pose increased risks to people. We look forward to Government providing more detail on:

- what the investment in ongoing monitoring will include;
- how it will be conducted; and
- how any changes in a country's approach or protections will be considered.

Redress requirements

126. The Government is proposing to clarify the legislation on redress. Redress mechanisms ensure that the law properly protects people, including when their data is transferred overseas. If people's rights are infringed, redress can provide compensation, other forms of relief or ensure enforcement. The current text is not clear whether redress should be judicial (eg provided for by a court of law or tribunal) or administrative (eg provided for by a regulator or ombudsperson). The Government is proposing to amend the legislation to make it clear that both types of redress are acceptable as long as the redress is effective (paragraph 254).

127. We welcome greater clarity and agree that it is important to ensure that any remedies are effective and legally binding, as appropriate. It is

important that the Government provides more detail on how they would assess whether redress mechanisms are effective.

3.2 Alternative transfer mechanisms

128. The Government is proposing to provide more ways for organisations to transfer people's data to countries not subject to an adequacy decision, while ensuring those people are appropriately protected (paragraph 257). Currently, data controllers exporting people's data to a country or jurisdiction not covered by adequacy regulations need to apply additional safeguards to protect people's rights and freedoms. The permitted safeguards are set out in Article 46 of the UK GDPR, and are known as alternative international transfer mechanisms (AITMs).

129. Currently, the most widely used AITM is standard contractual clauses (SCCs). This is a contract that organisations can use when transferring data to countries not covered by adequacy decisions. The ICO is currently consulting on replacing SCCs with the International Data Transfer Agreement[24] (IDTA), as part of a broader consultation on updating our approach to international transfers. This change is intended to take into account the binding judgment of the European Court of Justice in a case commonly known as "Schrems II". The ruling required organisations to carry out further diligence when making a transfer of personal data outside the UK to countries without an adequacy decision.

130. The consultation sets out the Government's proposals for developing AITMs to ensure they are proportionate, flexible, future-proof and interoperable.

Proportionality of appropriate safeguards

131. The Government is seeking to ensure that the safeguards applied during international transfers would be proportionate to the risks facing people in practice (paragraph 259).

132. As the consultation notes, achieving proportionate protection is complex. Currently, organisations must make a risk assessment before they may rely on an Article 46 UK GDPR transfer tool to make an international data transfer. This assessment considers the risk of the transfer tool that exporters put in place and the risks to people of making the transfer. A point of focus in this assessment is the destination country's legal regime, and whether it is sufficiently similar in objectives and purpose to the principles which underpin UK laws. Particularly, they need to consider

[24] ICO consults on how organisations can continue to protect people's personal data when it's transferred outside of the UK | ICO

those laws which might require that the importer gives a third party access to the data they receive. For example, this can include laws around surveillance for national security purposes.

133. International transfers should be focused on understanding, managing and mitigating the risk of the transfer being made. But as the consultation sets out and as we have heard through feedback from stakeholders, this process can be challenging for organisations, particularly small businesses. To address this the Government intends to clarify the legislation to reinforce the importance of proportionality when using alternative transfer mechanisms, and to ensure the ICO further supports organisations with guidance on determining risks (paragraph 259).

134. We agree that organisations would benefit from more support and guidance in this area, and that being able to efficiently and effectively transfer data is important for the UK economy. The ICO has already committed to providing guidance and tools to enable organisations to comply with the law and continue to enable data flows. As noted above, we are also currently consulting on a transfer risk assessment tool for use by data controllers, as part of our broader consultation on international transfers. We look forward to hearing stakeholders' feedback on the kinds of support they are seeking in assessing and mitigating risk.

135. As the Government looks to introduce a more proportionate approach to managing risks, it is important to consider where the responsibility for different aspects of the risk assessment should lie. The ICO can provide guidance on how to approach and conduct these assessments, and the kinds of safeguards that would be appropriate for different scenarios. Government will need to play a leading role in assessing the risks posed by the data protection regimes of specific countries, particularly for third party access to data. Given that accountability is a core principle of the data protection regime, it is also important that, while drawing on the increased guidance and support offered, data controllers remain accountable for their approach in practice. They must satisfy themselves that they are compliant with their responsibilities under data protection law and that the people whose data they are transferring are protected.

Reverse transfers exemption

136. The Government is proposing to exempt "reverse" transfers of personal data from international transfer requirements (paragraph 260). A reverse transfer is where data is received by a UK processor from overseas and is sent back to the original transferor, but is still considered a "restricted transfer". In other words, one where the UK data exporter needs to apply additional safeguards set out Article 46 of the UK GDPR. We support

changes which can reduce burdens in a proportionate way. As part of our current consultation on international transfers we include proposals on our interpretation of restricted transfers and the extra-territorial effect of UK GDPR. Depending on the outcome of this consultation, the effect of the revised guidance could reduce the number of issues that UK organisations face when making these reverse transfers. In other words, it could reduce the number of scenarios in which they are considered restricted.

137. Despite these potential changes, there would still be some scenarios where reverse transfers are still restricted. For example, those where data is being sent back to a controller covered by UK GDPR. Data flows are also complex, and it is likely to remain challenging for UK data exporters to identify where they can apply the proposed exemptions for reverse transfers. We encourage the Government to explore with data controllers how effective this exemption may be in reducing complexity.

Adaptable transfer mechanisms

138. The Government intends to make AITMs more flexible and increase inter-operability with other global regimes. They propose to do this by allowing organisations to create or identify their own alternative transfer mechanisms without approval by the ICO, in addition to those listed in Article 46 of the UK GDPR. This would replace the existing clause in Article 46(3)(a) which allows organisations to develop their own bespoke contractual clauses with ICO approval (paragraph 261).

139. We are supportive of providing organisations with the flexibility to develop mechanisms such as bespoke contracts, for which the ICO would provide guidance. Our draft International Data Transfer Agreement and Addendum to Standard Contractual Clauses already allows more flexibility and amendments than the EU Standard Contractual Clauses. Although these are still mandatory requirements for UK exporters.

140. Allowing organisations to create or adapt their own transfer mechanisms could deliver beneficial flexibility, as well as making it easier for new AITMs to adapt to new risks and businesses processes. However, there is a risk of inconsistent levels of protection. It is important that any new AITMs ensure the risks to people's data are appropriately assessed and mitigated and people's rights are upheld.

141. If organisations are allowed to create or adapt their own transfer mechanisms, consideration should be given to risk-based oversight of these mechanisms to help manage this risk. While not all bespoke AITMs would necessarily need regulatory approval, and some types of lower risk

transfers might be better supported by regulatory guidance, approval would be particularly important in higher risk transfers. More detail on the proposed approach would be helpful in exploring where this might be the case.

142. The role of the ICO would be important throughout the process of developing and deploying new AITMs. This includes ex ante (through guidance and templates, advice and consultation for the highest risk processing), and ex poste (providing oversight using our audit power and enforcement for the most serious cases of non-compliance). We therefore look forward to seeing further detail on how the Government would ensure the right balance is found between flexibility and assurance to create the appropriate regulatory oversight of this proposal.

143. Finally, given the current widespread reliance on SCCs and AITAs it is also important when considering developing new mechanisms that Government understands from stakeholders:

- why this tool is currently relied upon more than others; and
- what additional benefits for protection and businesses effectiveness can be gained from other mechanisms.

A power to create new alternative transfer mechanisms

144. The Government also proposes that the Secretary of State should be able to create or recognise new or additional transfer tools. We support the ability of the Government to create new mechanisms where these maintain the UK's high standards of data protection. We look forward to seeing further details of how this would work in practice.

3.3 Certification schemes

145. The Government is proposing a change to the current law to "allow certification to be provided for by different approaches to accountability". This is intended to increase the potential of using certifications as a international transfer mechanism by allowing more flexibility on how organisations demonstrate their accountability standards (paragraph 267).

146. Certification schemes, along with Codes of Conduct, are an important accountability tool. Currently, under UK GDPR as it is drafted, certification schemes can be applied to products or services to certify their compliance with data protection law. This can help provide certainty and assurance for people and businesses. A UK GDPR certification scheme is made up of three elements:

- the certification criteria – these form the set of requirements that conformity is assessed against (for data protection certification schemes these are the specific data protection requirements relating to the processing);
- specification of approved conformity assessment methods; and
- scheme rules for the management and operation of the scheme.

147. The ICO is responsible for considering whether criteria submitted to us by other bodies (such as standards bodies) are acceptable. These could be submitted to us on their own, or as part of a scheme. If the former, other organisations could then build on these criteria to create a scheme. We have a formal agreement with the UK Accreditation Service (UKAS), which is the UK's national accreditation body. It covers how we will work together to consider these elements, with the ICO focussing on the criteria, and UKAS the wider scheme. UKAS are also then responsible for accrediting CABs to those schemes, approving that they can certify organisations under the relevant scheme.

148. The current legislation sets out additional requirements for certification criteria to operate as international transfer mechanisms. These includes ensuring the certification provides binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including to protect people's rights. We will be publishing further guidance on the use of certification for international transfers later this year.

149. We are supportive of the Government exploring options that would better support certifications as an alternative transfer mechanism. Any new or additional types of schemes should not have a negative impact on the existing market, which is increasing in importance. There will also need to be clarity about the different types of certification available, and what these deliver. This is to prevent confusion among people and businesses about what is subject to certification. It is also important that Government ensures that the audit and assurance processes for these new types of certification are sufficiently rigorous to deliver high standards of data protection for people.

150. The Government also proposes that overseas bodies could be accredited as conformity assessment bodies (CABs) by the UK Accreditation Service (UKAS) (paragraph 268), for the purpose of developing international transfer schemes. This could potentially expand the available approaches available for firms to develop certification schemes to enable international transfers. We are supportive of exploring mechanisms that may make the

adoption of certification schemes as international transfer mechanisms work overseas. However, there are clearly challenges for firms to overcome to develop such schemes. So far we have not seen a strong market response based on the existing approach and the complexities are likely to remain a barrier, regardless of the approach taken to certification.

151. To ensure standards are upheld, accreditation of new CABs should continue to be subject to the appropriate UK regulatory oversight and provide an appropriate high level of protection for people. We encourage Government to gather further views and evidence from the bodies in question to test the viability of its proposals.

3.4 Derogations

Repetitive use of derogations

152. A derogation is a way that data controllers can make a transfer where the destination country is not covered by adequacy regulations and it is not possible to use an Article 46 transfer tool (AITM). There are specific criteria which must be fulfilled in order for such a transfer to take place and these form the set of derogations, which are set out in legislation.

153. As set out in the consultation, the available derogations are for situations where:

- the individual has given explicit consent for the proposed transfer after having been informed of the possible risks;
- the transfer is necessary for the performance of a contract between the individual and the controller, or pre-contractual measures taken at the individual's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the individual or of other persons, where the person is physically or legally incapable of giving consent; or
- the transfer is made from a register which according to domestic law is intended to provide information to the public and which is

> open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by domestic law for consultation are fulfilled in the particular case.

154. Accepted interpretation is that derogations should be used in exceptional circumstances. Currently Recital 111 states that the transfer must be "occasional" in relation to (b), (c), or (e). The legislation and associated case law also indicates that in each case reliance on the derogation must be both necessary and proportionate. The ICO's guidance is therefore that to rely on the derogations (other than "consent") the transfers cannot be "regular and predictable". The Government proposes establishing a proportionate increase in flexibility for use of derogations by making explicit that repetitive use of derogations is permitted (paragraph 270).

155. There is a fine balance to be struck here. Where transfers are repeated and predictable, there is an opportunity to put in place appropriate protections for people's data, through the use of an AITM. Where it is possible to put such protections in place, either wholly or in part, this should be done to ensure people are protected. It is important that any approach should emphasise the importance of having these protections in place, where and to the extent possible.

156. We acknowledge that there are situations where a transfer is repetitive, but it is not possible to put in place an Art 46 transfer tool (wholly or partly). In these scenarios, reliance on a derogation may still be "necessary and proportionate", and so the transfer should be allowed to go ahead. However, we also encourage Government to consider whether there are additional measures that could be put in place to help protect people in these circumstances. For instance, one option could be to require the data exporter to document the approach they have taken and the safeguards they have put in place. We are happy to work with Government further on this.

157. As noted above, one of the objectives of the proposed reforms to the transfer toolkit is to increase the flexibility and range of transfer tools available to organisations. This may therefore reduce the need for such flexibility to be granted through the use of derogations for repetitive transfers. It is therefore important to consider the benefits and potential risks of the proposals as a whole package.

158. Finally, we acknowledge that there may be a lack of clarity around the derogations, which may mean UK data exporters are reluctant to make certain transfers. We welcome any changes which would address this concern. We encourage the Government to seek evidence through the

consultation about whether there are other reforms that could make the appropriate use of derogations easier for organisations in practice.

Chapter four – Delivering better public services

4.1 Digital Economy Act 2017

159. Part 5 of the Digital Economy Act 2017 (DEA) is designed to reduce legal barriers to data sharing and enable public authorities to share personal data for specific purposes. The Government is exploring how to extend the public service delivery powers under section 35 of the DEA to business undertakings (paragraph 277). We support the aim of improving outcomes for businesses as well as for people and households so they can also benefit from joined-up public services across the digital economy, such as digital identity services.

160. We agree that data sharing can help public bodies and other organisations deliver modern, efficient services that make everyone's lives easier. We have worked closely with Government on the implementation of the data sharing measures in the DEA. We have also included references to the DEA in our statutory data sharing code of practice. We understand the benefits of data sharing enabled under the DEA. For example, in supporting people with multiple disadvantages and alleviating fuel and water poverty.

161. The powers to share information in the DEA come with a number of safeguards. This includes that all processing of information under these powers must comply with data protection legislation. The law is also supplemented by statutory codes of practice (the DEA codes). These must be consistent with the Information Commissioner's data sharing code of practice. It is important to consider whether any extensions of the powers and the additional data flows should be subject to the same or similar controls and assurances provided under the DEA.

4.2 Use of personal data in the Covid-19 pandemic

Private companies processing personal data to help deliver public tasks

162. The Government is proposing to clarify that private companies, organisations and people who have been asked to carry out an activity on behalf of a public body may rely on that body's lawful ground for processing under public task in Article 6(1)(e) of the UK GDPR rather than identifying a separate ground of their own (paragraph 282). This is in response to challenges faced during the Covid-19 pandemic.

163. The consultation states that relying on the legitimate interest lawful ground in Article 6(1)(f) has sometimes been complicated during the

pandemic. This is because the data controller is required to undertake an assessment of whether its own interests outweigh people's data protection rights, when often the wider public benefits of the processing are the main interest. Government does not believe that the onus should be on individual data controllers in the private sector to undertake legitimate interest balancing assessments when they have been asked to process personal data by government departments to assist them in the delivery of their public tasks.

164. It is relevant to clarify that it is not always necessary to rely on the legitimate interests lawful ground for these purposes. Under the existing data protection framework, if government requires controllers to carry out processing it may impose legal obligations to do so, in which case the legal obligation ground in Article 6(1)(c) would apply. Also in some instances a public authority may instruct a private sector organisation to process information on their behalf, in order to fulfil their public task. In these cases, the private sector organisation may be acting as a data processor, rather than a controller, in which case a separate lawful ground is not required.

165. Where it is necessary to rely on the legitimate interests lawful ground, the current legislation already permits data controllers to consider third party interests such as government promotion of public health. In such circumstances, the balancing test requires an assessment of whether those public health promotion interests are outweighed by people's rights. During the pandemic it was generally possible to find the balance in favour of the interests pursued by the government department or public body. It may be beneficial to explore ways in which further clarity can be provided about the breadth of the existing legitimate interest ground on the face of the legislation.

166. However, we also recognise that this can still be complex, particularly in cases where the private sector body has been asked to carry out the processing on behalf of the public sector. The consultation proposes that instead private sector bodies should be able to rely on a public authority's lawful ground for processing (paragraph 282), and that a public body may be required to clarify its powers or basis in law for directing the task.

167. The implication of this proposal is that the public authority, rather than the private sector organisation, would be accountable for determining that all relevant aspects of the public task lawful ground are satisfied. We would welcome clarification on this point. We also note that public bodies have checks and balances set out in their powers or other basis in law.

For example, they can be subject to specific confidentiality requirements, their decisions can be subject to judicial review and public officers can, in limited circumstances, be charged with misconduct in public office offences. These are important safeguards that help to ensure that the public authorities and officials are accountable and that the public interest is protected. Further clarity on the extent to which these would apply to private bodies in these circumstances is also important. The consultation also proposes applying this approach to organisations carrying out processing on behalf of law enforcement bodies. Clarity on the accountability and checks and balances in place is also required here.

168. It is also important to explain how the proposed approach protects people's data rights and does not lead to a reduction in these rights. For example, the right to object is a key data subject right. It is important to understand which organisation would be responsible for considering any objection where people chose to exercise this right. An organisation can refuse to comply with people exercising their right to object to their data being processed if they can demonstrate compelling legitimate grounds for the processing, which override people's interests, rights and freedoms. This is more complex in a scenario in which the organisation processing the data has not already conducted the balancing test.

169. We welcome the commitment that private bodies carrying out this kind of processing would not be allowed to continue to rely on that lawful ground to reuse the data for other purposes. We agree that this is an important safeguard. We also suggest that, where the private sector are carrying out processing of data on behalf of a public body, applying the same standard of transparency would be an important factor in building and maintaining trust. We therefore encourage the Government to extend freedom of information requirements to cover private organisations in these circumstances.

Processing health data in an emergency

170. The Government is proposing to clarify that public and private organisations may lawfully process health data when necessary for reasons of substantial public interest in relation to public health or other emergencies. This would be irrespective of whether the processing is overseen by healthcare professionals or undertaken under a duty of confidentiality (paragraph 286).

171. Under the current data protection framework, any data controller processing health data must satisfy a condition under Article 9 of the UK

GDPR. This is in addition to the legal ground for processing required under Article 6. This is because health data is special category data, which are types of data that are particularly personal or sensitive. Article 9 prohibits the processing of special category data, other than for the 10 listed exceptions to this general prohibition, usually referred to as "conditions for processing special category data"[25]. This list currently includes a condition for public health purposes, as long as there is oversight from a healthcare professional or the processing is carried out by a data controller acting under a duty of confidentiality.

172. We recognise the importance of being able to share health data in public health or other emergency circumstances. To this end, we note that under the existing regulatory framework, the Article 9 restrictions do not apply where "processing is necessary to protect the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent". Recital 46 provides further explanation of these provisions, confirming that "some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread".

173. The requirement for health data to be processed with the oversight of a health professional represents a safeguard for people. In particular, where the information being collected is complex and needs to be interpreted in order to use it in ways that affect them. We encourage Government to consider the implications of removing this safeguard completely. In particular, where it is difficult to predict the specific circumstances of a future emergency, and given government would have the option to legislate to permit processing in the particular circumstances, as they become clear.

174. However we recognise that health professional oversight is not always possible. This is why it is important that there is flexibility and an alternative for the processing to be carried out by someone owing people a duty of confidentiality. We welcome the commitment to ensuring that any changes would be time-limited and subject to appropriate safeguards reflecting the sensitivity of the data. However, we think it is important to retain the requirement for a duty of confidentiality as a minimum. This is vital to building and maintaining public trust in emergency situations. This

[25] More detail on the safeguards required is set out at What are the rules on special category data? | ICO

means that people are prepared to share their data and are confident that it will still be treated as confidential.

4.3 Building trust and transparency

Transparency mechanisms for algorithms

175. It is currently challenging for people or their representatives to understand:

- how AI systems are being used;
- how ethical and data protection considerations such as mitigating bias have been addressed;
- the approach to human oversight; and
- the level of risk associated with the algorithm.

176. We agree that there are clear benefits in strengthening transparency and clarity in this area. We think this would build trust in the use of algorithms in public sector decision-making and allow for greater levels of accountability. We welcome the Government's proposal to introduce compulsory transparency reporting on the use of algorithms in decision-making for public authorities, government departments and government contractors using public data (paragraph 290). We encourage Government to ensure the information provided in this reporting is both accessible and meaningful. We also encourage Government to consider how proactive publication mechanisms within FOIA and the EIRs could be used to support the implementation of proposals in this area.

Processing in the "substantial public interest"

177. Currently processing of special category data or criminal conviction and offence data can only take place in certain circumstances, known as conditions for processing. This is because the particular sensitivity of that data means additional protections are required. The UK GDPR and Schedule 1 to the DPA 2018 set out a range of situations when such sensitive data may be processed, and various tests or conditions that must also be met. The Government is considering whether to add to, or amend, existing conditions in Schedule 1 of the DPA to provide greater specificity (paragraph 293).

178. We appreciate that some organisations find it challenging to decide which of the conditions for processing applies. We recognise the benefits more clarity could bring, provided that appropriate safeguards are incorporated. We look forward to seeing further detail on this proposal as it develops.

179. The Government is also considering how to provide greater clarity for when controllers are required to demonstrate that processing is necessary for reasons of substantial public interest as part of satisfying a condition for processing (paragraphs 296 and 297). Two options are being explored. The first involves incorporating a definition of "substantial public interest" into the legislation. The second is to add to, or amend, the examples of specific situations that are already listed in Schedule 1 of the DPA as always being in the substantial public interest.

180. We agree with Government that any changes would need to be carefully considered to ensure sufficient transparency and a high level of protection for people, given the nature of the data involved. In our view, the first option, supported by regulatory guidance if necessary, may offer the most flexible solution, although we are interested in the views of stakeholders on this issue.

Clarifying rules on the police's collection, use and retention of biometric data

181. The Government proposes to clarify the rules on the police's collection and use of biometric data (paragraph 301). Whilst the existing legal framework is comprehensive, there is concern that it is complex and lacks transparency for both the police and the public in a fast-developing area. We welcome this ambition, as clarity is key to supporting the police in doing their job and maintaining high standards of data protection. The legislative framework includes data protection, law enforcement statute, the Protection of Freedoms Act (POFA 2012) and Biometrics Commissioner responsibilities under the Police and Criminal Evidence Act 1984.

182. Given this complexity, the Government is considering issuing additional codes of practice under Part 3 of the DPA in order to explain the application of data protection law in discrete areas. We recognise the benefits that codes of practice can bring for stakeholders, clarifying and explaining the requirements of the regulatory regime.

183. It is important to clarify who would be responsible for developing such codes of practice under Part 3 of the DPA. Also, to explain the legal status of such mechanisms, including in relation to the regulator and the courts. It is also important to ensure there is clarity on the distinction between these codes of practice, the data protection codes of practice the Commissioner was required to produce under the DPA, and codes of conduct. The latter are voluntary compliance mechanisms that can be

developed by trade associations or representative bodies on behalf of controllers and processors.

4.4 Public safety and national security

184. The DPA 2018 sets out the data protection framework in the UK, alongside the UK GDPR, and contains three separate data protection regimes:

- Part 2: sets out a general processing regime (the UK GDPR);
- Part 3: sets out a separate regime for law enforcement authorities; and
- Part 4: sets out a separate regime for the three intelligence services.

185. The Government wishes to standardise terminology and definitions across the different data processing frameworks in Parts 3 and 4 of the DPA, where appropriate (paragraph 305).

186. We are supportive of this where terms that are common to both regimes should carry the same meaning. However, if implementing such changes it would be important to recognise where and how the two regimes deliberately impose differing obligations on those processing under them. For example, people have more limited rights under the intelligence regime than where processing is carried out by competent authorities for law enforcement purposes. The extent of any changes would need to be very clear to prevent further confusion in an area that is already complex.

187. In addition the Government is suggesting that the provisions for joint controllership could be extended to enable cross regime controllers to collaborate more effectively (paragraph 306). Existing provisions in the legislation address when joint controllership arises. This is where two entities processing under the same regime jointly determine the purpose and means of the processing. However, they do not assist in improving working relations or data sharing between two entities. Where joint controllership exists, parties are able to determine their respective responsibilities for compliance with the requirements in the part of the DPA they are processing under. They may designate who will be the contact point for people.

188. The proposals about joint controllership are high level and further information is required to understand how such changes would be affected in practice. This is because entities are required to process personal data in accordance with the part of the DPA they are subject to.

In any more detailed proposals, we would want to guard against weakening the data protection regimes for policing and the intelligence services or introducing risks in the context of processing under Part 2 of the DPA.

Chapter five – ICO reform

189. This chapter of the Government's consultation sets out its intention to introduce reforms that would empower the Information Commissioner to protect data rights and promote trust in order to unlock the power of data. The consultation emphasises the importance of sustaining the ICO's world-leading reputation while preserving its independence.

190. We are supportive of these stated aims. We have highlighted earlier in our response that any package of reforms should, among other things, ensure the ICO continues to have the independence, powers and resources needed to fulfil our remit and to ensure the public has confidence that we are able to protect their interests. It is vital that any changes to the data protection framework take account of the continuing need for a strong regulator that is:

    - able to take action;
    - provide support to the regulated community and members of the public;
    - have international influence; and
    - deliver on the objectives set for it by Parliament.

191. Any changes must be considered in the context of ensuring that the ICO continues to be an effective regulator and with the aim of enhancing our ability to deliver these objectives.

192. Overall, we are broadly supportive of the proposed changes. We recognise that many of them are informed by work already underway at the ICO to align with corporate governance best practice. We welcome the recognition that the ICO is already on a transformation journey, enhancing our capacity and capability to ensure we continue to be a respected and influential regulator, with an agile and pragmatic approach.

193. We recognise that the continued evolution of the ICO is vital to the successful implementation of the reforms set out elsewhere in the consultation. We are supportive of a risk-based approach, with the dual purpose of proactive support and guidance, as well as supervision and enforcement. We believe that a strong ICO, with the right powers and responsibilities, is key to enhancing public trust in the way data is used, which underpins a successful and growing digital economy.

194. We note that the consultation references the ICO's role in regulating government and the public sector – under both data protection and access to information legislation. This, and our role as a rights based

regulator, is unique amongst the other regulators referenced in the consultation. This is an important consideration when determining the future governance model and appointment processes to key executive and non-executive roles. This is because the ICO needs to be, and be seen to be, independent from government in the exercise of its functions, especially in relation to freedom of information where we exercise a quasi-judicial function. We believe that the public expect public authorities to be held to a high standard when processing personal data, due to the nature and volume of this data. But also because there is often less choice about how and when information is shared with organisations delivering public services. It is therefore particularly important that there is an effective and independent regulator to hold government and other public authorities to account when this doesn't happen.

195. Independent oversight is increasingly being recognised as important internationally, including in agreements such as Convention 108+. It's importance has also been highlighted through previous jurisprudence. Maintaining an independent supervisory authority is therefore an important element of demonstrating that the UK has the high standards the international community expect, and which will be required for future global trade deal considerations and adequacy agreements.

196. We would welcome more specificity on how the proposed governance model and accountability mechanisms adequately preserve the ICO's independence to regulate the work of government. This is particularly relevant when considering the role of government in appointing Board roles, in particular the Chief Executive Officer, in setting strategic priorities and in the development of ICO guidance and codes of practice. In these areas, more detail on the specific checks and balances in place to ensure the ICO's continued effective delivery of this role would be helpful.

197. In considering the proposals about the reform of the ICO, we have taken account of both the wider context of the data reforms set out in the consultation and a set of guiding principles, as summarised below:

    - The need to ensure the ICO can deliver our responsibilities effectively.
    - The recognition that it is for Government and Parliament to set the regulatory framework and to define the role of an independent regulator. It would follow that the regulator is then able to act with independence within the legislative framework Parliament provides.

- The need for the ICO, as an independent regulator, to be fully accountable to Parliament for the effective discharge of its remit.
- The importance of recognising that the ICO's remit and mandate is broad and complex. This includes the necessity of safeguarding the independence required for the ICO's role in the oversight of government and the public sector, whilst also enabling the ICO to play an effective and trusted part alongside some of the UK's largest digital and economic regulators.
- The importance of the ICO's international role, where the UK's interests are best served by a strong, independent and respected regulator.

198. These principles are core to the continued success of the ICO, in the eyes of the organisations we regulate, as well as the public.

5.1 Strategies, objectives and duties

199. We are supportive of the ICO having clear statutory objectives. This approach would allow Parliament to clearly articulate the regulatory framework in which it wishes to see the ICO operate.

200. We welcome the recognition that we have developed our own strategic framework, through the Information Rights Strategic Plan and other supporting strategies. As well as being transparent about our regulatory priorities and approach to taking action and how we develop our policies and guidance. We also welcome the view that the ICO's primary objectives are to uphold data rights and to encourage trustworthy and responsible data use (paragraph 325). This reflects our stated aims in our current Information Rights Strategic Plan and ensures that our role in upholding public trust and confidence and people's data rights is clearly articulated in law.

201. A statutory requirement for the ICO to take into account such principles as economic growth, competition, public safety and regulatory co-operation (paragraphs 326 to 343) would, in our view, serve to enhance the clarity of purpose and accountability of the future ICO for our stakeholders. We welcome the recognition in the consultation of the ICO's crucial international role (paragraph 347), ensuring continued high standards of data protection for UK citizens and enhancing global regulatory cooperation. We will continue to develop our international strategy to enable greater transparency of our work in this area.

202. With regards to the specific objectives about competition and regulatory cooperation, we note the need to ensure that this is consistent with, and reflected in, parallel work to align the duties and powers of other regulators participating in the Digital Regulation Cooperation Forum.

203. Regarding regulatory cooperation, this duty would formalise our current approach to ensuring close working relationships with other regulators, as demonstrated through the recent ICO/CMA joint statement[26]. We recognise that it is important that regulators work in a joined-up way, with appropriate reciprocity. We would welcome consideration of how cooperation is enabled in other regulatory regimes. The requirement for other regulators to take privacy matters into account would allow for this concurrent working. Although it would be important to be clear about primacy, where multiple regulatory regimes are engaged in an issue. We would also welcome enhancements to how the ICO is able to share information with other regulators and believe that this would help to improve the effective cooperation between the ICO and our counterparts.

204. We recognise the distinction the consultation makes between operational and strategic priorities. We agree that, in order for the ICO to continue to function independently, particularly in relation to our regulatory interventions, we should be responsible for setting our own operational objectives and strategies (paragraph 344). This would ensure the ICO retains our independence from government in regulatory and organisational decision-making, allowing us to effectively discharge our duties as a UK regulator. This independence is also an important factor in preserving the ICO's international role and ability to influence on behalf of the UK government and its citizens and businesses to enhance trade and support cross border data flows.

205. Regarding the statement of strategic priorities (SSP), we note that while SSPs are commonplace amongst other UK regulators and are a helpful way of describing the regulator's role in the context of the wider public interest, it is critical that any SSP still enables the regulator to operate independently of government. The recognised need for the ICO to retain full discretion over its priorities is welcome. We note that is also in the interest of the Government for the regulator to maintain appropriate discretion when deciding how best to carry out its remit. We welcome the emphasis on the SSP forming part of the ICO's independent process of objective setting and the requirement for the ICO to formally respond to any SSP, rather than be bound by it (paragraph 346). It is our view,

[26] CMA-ICO joint statement on competition and data protection law - GOV.UK (www.gov.uk)

however, that it is for Parliament to set the ICO's objectives. In order to enhance the emphasis on independence in relation to the SSP, and in line with the principles set out above, consideration should be given to whether the SSP should be subject to Parliamentary approval. This would be in the same way as the ICO's Regulatory Action Policy and include an explicit exemption for the parts of the ICO's role involving oversight of government.

5.2 Governance model and leadership

206. We welcome the consultation's focus on ensuring that the ICO continues to deliver our increasingly important role effectively. We recognise the limitations of the Corporation Sole model, and we are pleased by the recognition in the consultation that the ICO has already made significant changes to our own governance structures, within the Corporation Sole model, to reflect good corporate governance practice.

207. We believe that the move to a Board and Chief Executive model, with a Chair appointed through a Crown Appointment and Letters Patent and titled the Information Commissioner (paragraph 353), would support the ICO in our aim to continue to be an effective and trusted regulator, fit for the future and able to work alongside the UK's largest economic regulators.

208. We welcome the continuation of the Information Commissioner title for the Chair of the Board (paragraph 356). This is an important aspect of retaining the ICO's international influence, vital for cross border data flows and trade. The continuation of the Crown appointment for this role (paragraph 358) is an important recognition of the ICO's unique role. We believe this is essential if the future ICO is to move away from a Corporation Sole governance model but retain responsibility for regulating government's use of personal data and its responsibilities under access to information law. We note, however, that the consultation is silent on removal from post of the Chair and other Board members and would benefit from clarity on the role government would have in this decision.

209. We recognise the value of considering the governance models of the other economic regulators in the appointment of Executive roles. However, there is a need to ensure that the unique role of the ICO in regulating government and the public sector, and the resulting need to maintain impartiality in doing that, is reflected in the proposals.

210. The current proposal for the Chief Executive to be appointed through a public appointments process (paragraph 359) would mean that the ICO

Board and Chair would not be responsible for the appointment of this role – the final decision would rest with Ministers. It should be recognised that this would then result in the ICO having a different model to that adopted by other economic regulators. For example, OFCOM, where the Chief Executive is a public appointment made by the OFCOM Board, with the approval of the Secretary of State. This proposal would, therefore, give the ICO a constitution less independent from government than that of other economic regulators, despite our role in overseeing the public sector and government.

211. It is our view that the ICO Board should be responsible for the appointment of Executive level roles, including the Chief Executive. We believe that as the Chief Executive is the most senior Executive on the Board, the Board should have the final decision about this appointment, rather than Ministers. In addition, as the non-Executive Chair would be a Crown appointee it is vital that they, and the Board, would have complete independence in making Executive appointments. There is provision for this approach in the governance code for public appointments, which sets out that "Ministers may, where they have the power to do so, choose to delegate responsibility for certain appointments to the appropriate body in question to run and make appointments[27]".

212. We recognise that government may wish to have a role in informing the appointment of the Chief Executive. However, in order to safeguard the independence of the appointment we recommend that the Secretary of State is consulted as part of a public appointment process, rather than the appointment being made by Ministers. This would ensure confidence in the future ICO's ability to regulate independently. This approach would align with OECD Best Practice Principles which state that "where there is a multi-member governing body, the CEO's primary accountability should be to the governing body, in order to safeguard the accountability of the CEO and independence of the regulator. The CEO should be appointed by, or on the recommendation of, the governing body[28]".

5.3 Accountability and transparency

213. We recognise the importance of accountability, particularly for an independent regulator. We support proposals that enhance the ICO's Parliamentary accountability. We are committed to being transparent about our goals, priorities and outcomes, including through KPIs and

[27] Microsoft Word - 20161216 Governance Code FINAL in CO template.docx (publishing.service.gov.uk)
[28] OECD Best Practice Principles for Regulatory Policy- The Governance of Regulators, p73

evaluation of our activities. We therefore welcome the proposed requirement for our Annual Report to report on performance against KPIs that are linked to a set of statutory objectives (paragraph 366).

214. Regarding other oversight mechanisms, the ICO has, in the past, always positively engaged with any review of our activities and performance. We have also undertaken independent reviews through our auditors, consultants or other third parties, where areas for development have been identified. We recognise that the power to commission an external review (paragraph 373) supports the principle of accountability. The clarification of this being a 'last resort' and the intention to introduce criteria for triggering a review are welcome, reducing the risk to the principle of independence.

5.4 Codes of practice and guidance

215. As the consultation acknowledges, we have developed a more consultative approach to guidance development. We welcome input into our policy development from a wide range of stakeholders. As such, the requirement to consult an expert panel (paragraph 379) aligns with our revised Regulatory Policy Methodology[29] and our current use of Technology, Legal and Children's Advisory panels. We agree that we should involve stakeholders in the development of our guidance and policy, as appropriate. This includes government, business, citizens, consumers and civil society groups. This approach would enhance the transparency of our policy making process while preserving the ICO's independence and is in line with our published Regulatory Policy Methodology.

216. It is however important, for both government and the ICO, that the ICO has complete independence when it comes to the final sign-off of any such products. The consultation currently proposes giving the Secretary of State the power to approve codes of practice and novel or complex guidance, and to require the ICO to prepare another version if it is not approved (paragraph 380).

217. With the principles of independence and accountability in mind, we recognise the value in guidance going through a robust development process to ensure consultation with affected stakeholders and businesses. This process already includes consultation with the Secretary of State on key pieces of guidance. In the case of statutory codes of practice, there is a legal requirement for the ICO to consult with the Secretary of State and

[29] regulatory-policy-methodology-framework-version-1-20210505.pdf (ico.org.uk)

for the Secretary of State to lay the final code before parliament for approval.

218. The ICO's regulatory guidance and codes of practice are a key aspect of how we exercise our regulatory functions. These proposals, which effectively amount to the right of veto for government over key pieces of guidance, have the potential to create a lack of clarity about the ownership and accountability for the content of the guidance. In our view, this undermines the role of the regulator and creates an increased risk of judicial review or challenge for both parties.

219. We note that elsewhere the consultation is rightly focused on parity with other UK regulators. It is our understanding that other regulators do not have comparable requirements for sign-off for their guidance. OFCOM and the FCA are only required to give notice of guidance, not to gain approval before publication. We are aware that the new Online Safety Bill contains some specific consultation and approval requirements for OFCOM about the guidance and codes of practice it will be required to produce. But these do not appear to be as extensive as those proposed for the ICO.

220. Finally, the introduction of a right of approval and veto of ICO guidance for the Secretary of State at the end of a process to develop, consult and then issue guidance may undermine the contributions of stakeholders to the development of the guidance. In fact it may create additional regulatory uncertainty for business, as well as operational uncertainty for the ICO.

221. It is our view that this proposal is fundamentally at odds with safeguarding the ICO's independence, which is key to engendering the public's trust and confidence in the digital and data economy.

5.5 Complaints and Enforcement powers

222. We welcome the consultation's recognition of the ICO's increased focus on 'upstream' or proactive support and guidance for organisations. We believe that ensuring compliance is the best way to deliver outcomes for the public and appreciate proposals that support this approach. We are focused on delivering our responsibilities in a way that both provides value for money for our fee payers, but also tangible outcomes for our customers, wherever possible.

223. It is our understanding that the proposed approach of requiring an organisation to attempt to resolve complaints before referral to the regulator (paragraph 384) would afford members of the public the best

opportunity to receive the information they require without recourse to a third party. The proposals also include a requirement for organisations to have a simple and transparent complaints-handling process in place. This is not mandatory under the current data protection regime (paragraph 386). Organisations would also be required to be more transparent by publishing information about the type and volume of complaints they receive. Requiring organisations to report on their compliance in this way, as they must in other areas of regulation (for example health and safety or equality) is a positive tool to drive market led compliance. Although we recognise that there is a need to limit any burdens on small or low risk organisations.

224. An additional benefit of this process would be that any further explanation could be sought by and provided to the person making the complaint prior to an issue being reported to the regulator. This would allow for the dispute to be clearly defined, with a final review outcome being shared that would also serve as the final response from the organisation that the ICO could assess. All parties would have had an opportunity to fully articulate the concerns and for those concerns to be fully and formally answered.

225. Government proposes to introduce a list of criteria by which the ICO can decide to not investigate a complaint (paragraph 387). While this would enhance the ICO's discretion in dealing with complaints, this would need to be carefully defined to ensure people's rights are not adversely affected. Finally, we would recommend considering giving the ICO the power to make recommendations to a data controller following a complaint about how best to resolve it. This would ensure that, where appropriate, complaints from the public lead to tangible outcomes, which is often what they tell us they want by raising their complaint in the first place.

226. The proposed additional powers on technical reports (paragraph 394), compelling witnesses to interview (paragraph 399) and penalty notices (paragraphs 405 and 406) would support our work to supervise and implement the regulatory framework set by Parliament. We welcome these proposals.

227. The power to commission an independently produced technical report, as the consultation notes, would be similar to the power the Financial Conduct Authority (FCA) has under the Financial Services and Market Act

(s.166)[30]. Used in a risk-based, proportionate manner this would support our ability to fully and efficiently investigate concerns and ensure we are identifying and mitigating both current and future risks to people. This would be particularly important for incidents involving the UK's critical national infrastructure. Use of this power would not be necessary in scenarios where organisations are well-informed about the technical factors underlying the incident and are willing to share information to cooperate with and support our investigations. However, we do anticipate this would be of benefit in cases where a company is either not prepared to cooperative with the ICO, or not sufficiently informed to manage future risks. Regarding the cost of producing a report, we note that similar provisions in the Irish Data Protection Act 2018 (section 135 (10)) require the data controller or processor to meet the costs of preparing reports.

228. The power to compel an individual to answer questions would ensure meaningful cooperation with our investigations. The power is intended to enable the effective gathering of evidence, and thus a more robust resolution to the investigation. As the consultation notes, this power is not novel and is utilised by a range of other regulators. This includes the CMA (under s.26A of the Competition Act 1998[31] and s.193 of the Enterprise Act 2000[32]), as well as the FCA (under s.171 of the Financial Services and Markets Act 2000[33]), who like the ICO investigate complex and technical cases. Of course, the ICO supports having due regard to people's fundamental rights and due process.

229. The proposal to amend the statutory deadline for the ICO to issue a final penalty notice following a Notice of Intent (NOI) from six to 12 months, and the provisions to stop the clock where information is not provided on time, would ensure that the ICO has sufficient time to investigate some of our more complex cases and properly consider any representations made by the parties under investigation.

230. It is our view that the range of proposals set out in the consultation would enhance the efficiency of our investigations by enabling the ICO to more quickly establish the facts of the case and would bring our powers in line with the economic regulators. We also welcome the formalisation of some of the current transparency and accountability mechanisms in place during the investigation process. For example, setting out timescales at

[30] Financial Services and Markets Act 2000 (legislation.gov.uk)
[31] Competition Act 1998 (legislation.gov.uk)
[32] Enterprise Act 2002 (legislation.gov.uk)
[33] Financial Services and Markets Act 2000 (legislation.gov.uk)

the start of the investigation and reporting on the time taken to conclude investigations.

5.6 Biometrics Commissioner and Surveillance Camera Commissioner

231. We agree that clarity about regulatory remits is crucial in areas such as police use of biometrics and overt surveillance. We note the intention to build on existing efforts to simplify the regulatory landscape (such as the recent appointment of one Biometrics and Surveillance Camera Commissioner) by assessing the feasibility of combining these functions and absorbing them into the ICO's remit (paragraph 410). We recognise the benefits of this approach for stakeholders in these two areas and see the close alignment of the work with our existing responsibilities. We are open to this expansion of our regulatory remit, subject to appropriate funding, and await further detail on how any transfer of functions would work in practice.

5.7 Resourcing the ICO

232. While there are no specific proposals about the funding of the ICO in the consultation, we welcome the intention to assess the impact of the proposed changes on the services the ICO provides and what, if any, changes in resourcing would be needed.

233. It is clear that, if the proposals were implemented as set out in the consultation, there would be a significant impact on the way the ICO delivers our work. As the consultation recognises, the ICO is committed to investing in our future looking functions, to ensure we have the intelligence and research capability needed to identify emerging issues, allowing for early intervention where there may be potential harm, but also to spot opportunities to enhance people's rights and promote innovation and growth. Our ability to do this would be enhanced by some of the proposals that would allow us to devote more resources to horizon scanning and proactive functions, which in turn would ensure better outcomes for members of the public and value for money for fee payers.

234. However, there are several areas where additional capacity and capability would be required to ensure the ICO could successfully deliver the requirements of a new data protection framework. Without changes to the legislative framework, which would reduce the number and nature of the reactive statutory obligations placed on the ICO, the substantial increases in proactive responsibilities currently described in the consultation represent a potentially significant risk to ICO capacity. As such, we would

welcome a more detailed impact assessment on the overall cost to the ICO, and therefore fee payers, of any changes to the services the ICO is required to deliver.