Department for
Digital, Culture
Media & Sport

Data: A new direction

10 September 2021

Ministerial foreword

Data is now one of the most important resources in the world. It fuels the global economy, drives science and innovation, and powers the technology we rely upon to work, shop and connect with friends and family. Now that we have left the EU, we have the freedom to create a bold new data regime: one that unleashes data's power across the economy and society for the benefit of British citizens and British businesses whilst maintaining high standards of data protection. As Digital Secretary, achieving this goal is one of my Ten Tech Priorities.

Today's publication of the Government's proposed reforms is a key milestone in that journey. They build on the current regime - aspects of which remain unnecessarily complex or vague, and which continue to cause persistent uncertainty over three years after its introduction. Our ultimate aim is to create a more pro-growth and pro-innovation data regime whilst maintaining the UK's world-leading data protection standards.

The reforms outlined in this consultation will:

- strengthen our position as a science superpower, simplifying data use by researchers and developers of AI and other cutting-edge technologies
- build on the unprecedented and life-saving use of data to tackle the COVID-19 pandemic
- secure the UK's status as a global hub for the free and responsible flow of personal data - complementing our ambitious agenda for new trade deals and data partnerships with some of the world's fastest growing economies
- reinforce the responsibility of businesses to keep personal information safe, while empowering them to grow and innovate
- ensure that the ICO remains a world-leading regulator, enabling people to use data responsibly to achieve economic and social goals

The protection of people's personal data must be at the heart of our new regime. Without public trust, we risk missing out on the benefits a society powered by responsible data use has to offer. And far from being a barrier to innovation or trade, we know that regulatory certainty and high data protection standards allow businesses and consumers to thrive.

These reforms will keep people's data safe and secure, while ushering in a new golden age of growth and innovation right across the UK, as we build back better. They are part of our wider work on digital

technology - building on our ground-breaking Digital Regulation Plan and Online Safety Bill. They also align with our plans to drive forward ambitious data adequacy agreements with other leading economies - and I hope you will all join me in supporting this work.

Rt Hon Oliver Dowden CBE MP
Secretary of State for Digital, Culture, Media and Sport

Table of contents

Introduction

1. The government wants to secure an even better data protection regime that fully supports a world-leading digital economy across the UK. As set out in the National Data Strategy, data is a strategic asset and its responsible use should be seen as a huge opportunity to embrace. Unlocking the power of data is one of the government's 10 Tech Priorities.

2. Outside of the European Union, the UK will capitalise on its independent status and repatriated powers to operate a pro-growth and innovation-friendly regime that maintains its high data protection standards. The government intends to leverage the UK's existing strengths and progressive values, as well as the competence and pragmatism of its regulatory institutions, to respond more agilely to a rapidly developing digital economy and society that are fuelled by data.

3. Responsible use of data is also a key enabler of the government's work to build back better, just as it was a cornerstone of the nation's fight against Coronavirus (COVID-19). The response to the COVID-19 pandemic showcased how the government and organisations can share and use personal data responsibly to develop vital services that keep people safe and save lives. However, it also highlighted some shortcomings of our current data regime: the right ways to share data can be complex to identify and apply quickly, and some existing rules and guidance are either too vague or overly prescriptive.

4. Innovative uses of personal data are at the forefront of driving scientific discovery, and enabling cutting-edge technology, like artificial intelligence (AI). The government wants to realise these innovations in a responsible way so that they bring real benefits to people by improving lives, creating jobs and helping to create a fairer society. This means maintaining a clear legal framework overseen by a regulator that takes account of the benefits of data use, while protecting against the harms that can come from using personal data irresponsibly.

5. The Information Commissioner's Office (ICO) is one of the UK's most important regulators with a remit covering many organisations across most parts of our economy and society. As use of personal data has become more widespread, the ICO has taken great strides in recent years to build its capability and guide organisations that want to use data safely and securely. It is important that the ICO's legal framework supports these goals, allowing the regulator to focus more on preventing harmful uses of data as early as possible but also to take account of the impacts of not realising the full benefits of using personal data responsibly.

6. Global trade, scientific cooperation, national security and law enforcement cooperation are all underpinned by data flowing across borders. We must ensure people's data is protected in line with our values when sent to other jurisdictions and remove any unnecessary impediments to international data flows that would limit growth, productivity, security and our ambitions for Global Britain. The government also recognises the importance of maintaining interoperability between the UK's regime and other regimes, built on a shared international understanding of the underlying principles of data protection in order to create a coherent environment for businesses seeking to operate internationally.

Our Approach

7. In September 2020, the government published an ambitious new National Data Strategy, launching a nationwide conversation about how to make the most of data's many opportunities. We want to continue that dialogue and, building on the high watermark of data use set during the COVID-19 pandemic, establish a data protection regime that will:

a. Support vibrant competition and innovation to drive economic growth

b. Maintain high data protection standards without creating unnecessary barriers to responsible data use

c. Keep pace with the rapid innovation of data-intensive technologies

d. Help innovative businesses of all sizes to use data responsibly without undue uncertainty or risk, both in the UK and internationally

e. Ensure the ICO is equipped to regulate effectively in an increasingly data-driven world

8. This will deliver better outcomes for people. The UK public will benefit from better use of personal data, which will deliver a stronger economy, more efficient and effective public services, and greater innovation in science and technology. People will also be able to have trust in how their data is being used, as we shift the regulatory regime away from ineffective processes towards greater accountability on organisations to use data responsibly. This shift will be supported by a more risk-focused regulator that can identify and tackle potential harms more quickly.

9. Data-driven organisations will also benefit from better outcomes. The regulatory regime will be clearer and more suited to an agile, technology-driven economy. Regulatory requirements will be focused on the outcomes that must be achieved, rather than prescribing how they are achieved. The UK's regime will also be designed to operate globally, recognising that our most successful organisations work and transfer data across borders.

10. To this end, a set of principles guide the proposals set out in this consultation:

a. The UK's data protection regime should create a net benefit for the whole of the UK, unlocking new economic opportunities both at home and abroad, and keeping our society safe and secure

b. The UK's data protection regime should be future-proofed with a responsive framework that enables responsible innovation and a focus on privacy outcomes that avoids imposing any rules today that become obsolete as the technological landscape evolves

c. The UK's data protection regime should deliver a high standard of data protection for citizens whilst offering organisations flexibility in determining how to comply most effectively

d. Organisations that comply with the UK's current regime should still be largely compliant with our future regime, except for only a small number of new requirements

e. The government's approach to data protection should actively take into account the benefits of responsible use of personal data, while proactively maintaining public trust in such uses

f. Effective, risk-based and preventative supervision is critical to realising a pro-growth and trusted data regime, and the ICO's world-leading status as the UK's independent data protection regulator should be sustained

11. The reforms presented below for consultation deliberately build on the key elements of the current UK General Data Protection Regulation (UK GDPR), such as its data processing principles, its data rights for citizens, and its mechanisms for supervision and enforcement. These key elements remain sound and they will continue to underpin a high level of protection for people's personal data and control for individuals over how their data is used. Organisations have invested in understanding, complying with and implementing this regime, and the ICO's toolkit for supervision is fundamentally fit for purpose. The reform proposals offer improvements within the current framework, while maintaining the UK's worldwide reputation for high data protection standards and securing public trust.

International Context

12. Our hyper-connected world is increasingly reliant on international flows of personal data, which underpin so much of our economic activity, as well as vital scientific research, effective law enforcement cooperation, national security capabilities, and the delivery of public services.

13. An important consideration for international flows of personal data to and from the UK are the rules that facilitate the safe transfer of personal data to the European Union. The UK was a longstanding proponent of high data protection standards while part of the EU, and it will remain so as an independent nation, leading the way in creating the best possible data protection regime that exists globally. Recently, the UK and our European friends and partners agreed that our respective data regimes offer high enough standards of data protection for personal data to flow between our jurisdictions without any additional safeguards - that is, the existing safeguards in our regimes are mutually adequate for the protection of personal data. The UK has also provisionally recognised the regimes of other EEA member states as adequate, pending the full adequacy assessments which will be completed over the coming years.

14. Looking ahead, there are lively debates worldwide about the future of data protection, spurred by the pace of sweeping technological change, especially in data-intensive sectors. These debates are occurring within the EU, after more than three years' experience of implementing the GDPR.[1] The GDPR has applied in the UK since 2018, supplemented by the Data Protection Act 2018, and was incorporated into UK law as the UK GDPR at the end of the Brexit transition period.[2] The government recognises that different jurisdictions operate different data protection regimes, which reflect the specific values and priorities of their societies. Respect for the existence of multiple different data protection regimes and recognition of the importance of striving towards increased interoperability to support trusted international flows of data are key parts of the UK's approach.

15. In that spirit, the government believes it is perfectly possible and reasonable to expect the UK to maintain EU adequacy as it begins a dialogue about the future of its data protection regime and moves to implement any reforms in the future. European data adequacy does not mean verbatim equivalence of laws, and a shared commitment to high standards of data protection is more important than a word-for-word replication of EU law. Indeed, other countries, such as Israel, have been granted adequacy decisions by the EU while pursuing independent and varied approaches to data protection, reflecting their unique national circumstances, cultures and heritages.

[1] Javier Espinoza, Financial Times, 'EU must overhaul flagship data protection laws, says a 'father' of policy'
[2] COM(2020) 264 final, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation'.

16. The government recognises the value of positive adequacy decisions in allowing personal data to be transferred without any additional safeguards between the UK and adequate third parties. Adequacy decisions are just one mechanism to enable international data transfers, however. Many alternatives exist, some of which are widely used already. To support trusted data flows across the world, these alternative mechanisms, such as Standard Contractual Clauses (SCCs), must continue to be readily available, flexible and straightforward to implement. The government will continue to improve the design of alternative data transfer mechanisms, alongside further engagement with international partners to ensure the global regulatory framework enables trusted, free flow of data.

Overview of Consultation

17. This consultation is the first step in delivering on Mission 2 of the National Data Strategy to secure a pro-growth and trusted data regime. The government is committed to working with partners across all sectors and parts of the UK to secure an even better data regime and it has already engaged with the ICO.

18. This consultation is the first step in the process of reforming the UK's regime for the protection of personal data. Consultation responses will provide evidence to help shape any future reforms. Throughout this consultation, the government welcomes views on its proposals and further opportunities to create an even better data protection regime.

19. The government is taking an evidence-based approach to developing these proposals. Our initial economic analysis shows that our reform package will have a net direct monetised benefit of £1.04 billion over 10 years, even after accounting for potential costs incurred through any future changes to the UK's EU adequacy decisions. This is driven by unlocking more research and innovation, while easing the cost of compliance for businesses. This is before accounting for the potential benefits to UK trade, although these impacts can be difficult to quantify. Further details on our analysis and modelling assumptions can be found in the draft impact analysis published alongside this consultation.

20. The reform proposals will also offer further benefits that are more difficult to quantify in economic terms. For example, the proposals in Chapter 1 on clarifying the circumstances in which data can be processed for legitimate interests could give data controllers greater confidence to process data for law enforcement and safeguarding purposes, for example, with benefits for the wider public. The proposals in Chapter 4 should lead to better data-sharing between public authorities and increased transparency of their processing activities should lead to more effective delivery of public services and higher levels of public trust.

21. These proposals will also enhance the ability of our law enforcement agencies and UK Intelligence Services to protect public safety and national security. This reform agenda can reduce differences and improve consistency across the general, law enforcement and national security frameworks for data processing. It will provide greater legal clarity and increase public confidence in the sharing of data processed in the public interest, including for law enforcement and national security purposes.

22. The government is giving due consideration to the public sector equality duty, under the Equality Act 2010, as it develops these proposals. The government believes that proposals to, for example, enable organisations to process personal data for the purpose of monitoring and mitigating bias in AI systems may help to reduce inequality. The government is preparing a full

public sector equality duty assessment for these proposals and would also welcome views on the extent to which any of the reform options below may have an impact under the Equality Act 2010.

23. Finally, the government expects to influence the international debate on data protection and the design of data protection regimes in other jurisdictions. The UK will advocate globally for the principles that drive our proposed reforms to be adopted by international partners who share our values and seek to maximise the potential of responsible data use. Further benefits will flow to the UK, as well as globally, if these principles are more broadly adopted, leading to better and more interoperable data protection regimes in other jurisdictions.

24. Responses to this consultation will help to shape any future reforms. Views are also sought on a number of emerging policy areas on which further evidence will help to build and assess the case for legislative change. Details on how to respond, including the length of the consultation period, are at the end of this document.

Chapter 1- Reducing barriers to responsible innovation

1.1 Introduction

25. Data is the driving force of the modern economy. Our approach to data therefore affects the ease, costs and risks of developing new technologies and services.[3]

26. There is huge potential for linkage and re-use of datasets across organisations, domains and sectors in order to enhance the development and commercialisation of new products, services and solutions, and to deliver wider public benefits.[4] The right governance, regulations and incentives will encourage organisations to make use of data responsibly.

27. The UK GDPR provides an important regulatory framework for access, use and re-use of personal data that protects the rights of individuals. It also provides rules that facilitate data sharing in ways that are accountable, lawful, fair and secure. The government is committed to maintaining high standards of data protection so that people have confidence in the use of their personal data.

28. Looking ahead, the government recognises that any data protection regime requires active interpretation and application to new and emerging technologies. The UK's data protection regime should be an adaptable and dynamic set of rules that are flexible enough to be interpreted quickly and clearly in order to fit the fast-changing world of data-driven technologies.

29. With the support of the ICO, organisations have been learning how to apply the UK GDPR to their data processing activities and new data-driven technologies over the last three years. This is an important and ongoing process that is not without challenges: there is complexity both in regulatory concepts and rules, and the huge variety of data processing activities to which they should apply. Persistent uncertainty about how to operationalise our data protection regime risks creating barriers to data access, use and sharing that stifle innovation and competition.

30. The government has heard from stakeholders that elements of the law can create barriers to responsible innovation. Some definitions are unclear and lack explanatory case law or regulatory guidance that could take years to develop; organisations may choose not to use data as fully as they could owing to unfounded concerns about legality. For example, the rules for some organisations to use and to re-use personal data for research are difficult to navigate, despite the public being generally in favour of their personal data being used for scientific research that can deliver real benefits to society.[5] The government has also heard evidence that uncertainty about when different lawful grounds for processing personal data should be used has led to an over-reliance on seeking consent from individuals. This creates an unnecessary burden for consumers as well as for organisations. Finally, the increasing adoption and potential of new data-driven technologies is dependent on clear and consistent rules about the use of personal data.

31. Providing greater clarity in our data protection legislation is an important step to ensure that our laws keep pace with the development of cutting-edge data-driven technologies. The potential reforms set out in this chapter are necessarily technical in nature. They are intended to create more certainty for organisations about when and how they can responsibly use personal data,

[3] DCMS: 'Data-enabled trade analysis using UNCTAD's classification of digitally-delivered trade to calculate data-enabled trade', 2019
[4] Public Health Research Data Forum: 'Enabling Data Linkage to Maximise the Value of Public Health Research Data', 2015
[5] DCMS, Statistical data set, Ad-hoc statistical analysis: 2020/21 Quarter 2, 9 July 2020

and to ensure our laws more accurately reflect people's views about how they expect their data should be used and when they should actively give consent.

32. A further source of ambiguity and potential confusion is the legislative design of our existing regime. The UK GDPR incorporates a large number of recitals that act as an explanatory or interpretative guide to the articles of the legislation. They offer information about the intended scope, purpose or effects of the law, which are valuable for understanding how it should operate in practice. The recitals do not, however, form part of the operative text in legal terms and their contents are not fully mirrored in the main body of the UK GDPR. Consequently, organisations may be reluctant to adopt an interpretation of the legislation that relies on a reading of the recitals that is not supported by an appropriately literal reading of the operative text, even if such an interpretation is likely to be in keeping with the intent of the law. To address this, the government proposes to transfer certain recitals into the articles of the legislation itself.

33. Proposals to provide greater clarity in legislation will complement the ICO's ongoing work to offer guidance and support about how to apply the rules. This will help innovators achieve their goal of creating the next wave of ground-breaking data-enabled products and services in ways that preserve public trust.

1.2 Research Purposes

34. The UK is ranked second in the world for science and research, and 54% of our output is world-leading. Personal data lies at the heart of a wide range of research activities across many sectors, spanning international networks of researchers. The sharing of scientific data with international partners helps to advance research in the UK and global capacity building in areas such as climate, biodiversity and health.[6]

35. The importance of personal data in research activities to our economy and wider society is reflected in the UK GDPR. The legislation provides specific allowances and derogations in relation to processing for archiving purposes in the public interest, scientific or historical research and statistical purposes (defined more generally in this chapter as 'research purposes'), which are designed to make it easier for researchers to:

    a. Re-use personal datasets for different research projects, subject to safeguards such as techniques that make it less easy to identify individuals from data sets (generically known as pseudonymisation techniques)[7]

    b. Retain personal datasets, and maintain their integrity and utility[8]

36. Both the UK GDPR and the Data Protection Act 2018 provide additional safeguards for research purposes to ensure that individuals' rights are given a sufficient level of protection. These safeguards include:

    a. Article 89(1) UK GDPR, which provides that processing for research purposes shall be subject to appropriate safeguards, including technological and organisational techniques which may include pseudonymisation

[6] European Academies, Science Advisory Council, 'International Sharing of Personal Health Data for Research', April 2021
[7] Article 5(1)(b) and Article 89(1) UK GDPR
[8] Article 5(1)(e) UK GDPR

b. Section 19 Data Protection Act 2018, which provides that processing for research purposes will not meet the criteria in Article 89(1) of the UK GDPR if it is carried out for making decisions about data subjects (unless for approved medical research) or it is likely to cause substantial damage or distress to a data subject

37. In the immediate term, the government welcomes the guidance that the ICO is developing to provide greater clarity for researchers on the various research provisions in the legislation and when they apply. However, the structure of the current legislation makes it difficult to realise the full benefits of this system. This cannot be solely addressed by improved guidance. Through this consultation the government seeks to understand how current legislation could be amended to support responsible research activity using personal data.

38. Relevant provisions are dispersed across the existing legislation and many important issues, as set out below, are only broached by the recitals to the UK GDPR rather than its operative text, which creates interpretative ambiguity. The difficulties in navigating these provisions can be understood in four broad categories:

39. Structure: provisions for research are complex, dispersed and layered both within the UK GDPR and Data Protection Act 2018. Navigating this web is a demanding task but a vital one for researchers to determine their legal obligations and whether any exemptions could apply. This complexity creates both real and perceived barriers for organisations.

40. **To address this problem, the government is proposing to consolidate and bring together research-specific provisions**, bringing greater clarity to the range of relevant provisions and how they relate to each other.

The government welcomes views on the following question:

Q1.2.1. To what extent do you agree that consolidating and bringing together research-specific provisions will allow researchers to navigate the relevant law more easily?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

41. Scope: there is no definition of 'scientific research' in the operative text of the UK GDPR. Recital 159 to the UK GDPR provides a definition of scientific research purposes which includes, for example, technological development and demonstration, fundamental research, applied research, privately funded research and studies conducted in the public interest in the area of public health. This definition is intended as an interpretive aid, however, and does not have the same legal status as the operative provisions. Reducing uncertainty around what constitutes research would reduce the perceived level of risk to organisations, and also improve transparency for individuals.

42. **The government therefore proposes to incorporate a clearer definition of 'scientific research' into legislation.**

The government welcomes views on the following questions:

Q1.2.2. To what extent do you agree that creating a statutory definition of 'scientific research' would result in greater certainty for researchers?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q1.2.3. Is the definition of scientific research currently provided by Recital 159 of the UK GDPR ('technological development and demonstration, fundamental research, applied research and privately funded research') a suitable basis for a statutory definition?

- *Yes*
- *No*
- *Do not know*

Please explain your answer, providing supplementary or alternative definitions of 'scientific research' if applicable.

43. Access to data: 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. Each lawful ground has its own conditions that must be fulfilled, and the lawful ground that is suitable for one researcher may not be for another. Uncertainty around determining lawful grounds could hinder or discourage important research.

44. **The government is considering the following two proposals to tackle the challenge of determining the best lawful ground to apply to the use of personal data for research purposes**:

a. **Clarifying in legislation how university research projects can rely on tasks in the public interest (Article 6(1)(e) of the UK GDPR) as a lawful ground for personal data processing.** At present, universities are identifying a legal basis to use for research in an unclear and inconsistent way. Uncertainty may be creating burdens or discouraging useful research. Clearly defining when universities can rely on Article 6(1)(e) of the UK GDPR may reduce these burdens and increase transparency for data subjects on how universities are using personal data.

b. **Creating a new, separate lawful ground for research, subject to suitable safeguards.** A new lawful ground could help reduce the complexity for organisations undertaking research in identifying a legal ground but would require safeguards on top of

those already present in Article 89(1) of the UK GDPR in order to prevent a data subject's personal data from being used in unexpected ways.

The government welcomes views on the following questions:

Q1.2.4. To what extent do you agree that identifying a lawful ground for personal data processing for research processes creates barriers for researchers?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible, including by describing the nature and extent of the challenges.

Q1.2.5. To what extent do you agree that clarifying that university research projects can rely on tasks in the public interest (Article 6(1)(e) of the UK GDPR) as a lawful ground would support researchers to select the best lawful ground for processing personal data?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q1.2.6. To what extent do you agree that creating a new, separate lawful ground for research (subject to suitable safeguards) would support researchers to select the best lawful ground for processing personal data?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q1.2.7. What safeguards should be built into a legal ground for research?

45. Re-use (further processing) of personal data: re-using personal data (also known as 'further processing' of personal data) for a separate purpose to that for which it was first collected can facilitate innovation in the delivery of products and services across both private and public sectors.

46. The current legislation acknowledges the value of sharing personal data amongst the research community for further processing in two broad ways. First, the recitals to the UK GDPR recognise it is often not possible to fully identify the purpose of processing of personal data for a research project at the time of data collection.[9] The recitals suggest that data subjects could give 'broad consent' to processing of personal data for certain areas of scientific research when in keeping with recognised ethical standards for scientific research.[10] By providing broad consent, a person consents to their data being used not only for a narrow, specified research purpose, but for broader areas of scientific research. However, the suggestion in the recitals is not reflected in the relevant operative provisions for the use of consent as a lawful ground for research purposes. Moreover, there is uncertainty about the concept of broad consent and how to reconcile it with the standards for valid consent as a lawful ground for data processing, whereby consent must be freely given, specific, fully informed and unambiguous. In a research context, the nature of processing activities may not be fully determined at the outset, limiting the extent or specificity of information available to the data subject. The recitals recognise therefore that a broader form of consent may be appropriate.

47. Second, Article 5(1)(b) of the UK GDPR confirms that further processing for scientific or historical research purposes, archiving in the public interest and statistical purposes will always be compatible with the original purpose for which the personal data was collected. However, while the recitals provide more clarity by stating that research purposes are 'compatible lawful processing operations', the operative text does not state explicitly that further use of data for research purposes passes the lawfulness test under Article 6 of the UK GDPR.

48. **The government proposes clarifying in legislation that data subjects 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. The government also proposes 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.**

The government welcomes views on the following questions:

Q1.2.8. To what extent do you agree that it would benefit researchers to clarify that data subjects 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?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

[9] Recital 33, UK GDPR
[10] Ibid.

Q1.2.9. To what extent do you agree that researchers would benefit from clarity that further processing for research purposes is both (i) compatible with the original purpose and (ii) lawful under Article 6(1) of the UK GDPR?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

49. The government is considering whether a further amendment to legislation would be valuable with respect to the transparency requirements for re-using personal data for research purposes. Further processing of personal data might be limited by an imbalance between researchers who collect personal data directly from data subjects and those who collect personal data indirectly:

    a. Article 13(1) and (2) of the UK GDPR require that important information be provided to the data subject at the point of collection. This information includes the identity and the contact details of the controller, the purposes and legal basis of the data processing for which the personal data are intended, and notification if the data will be transferred to third parties.

    b. Article 13(3) of the UK GDPR requires the data controller to provide additional information to the data subjects if they intend to further process personal data for a purpose other than that for which the personal data were originally collected. Research processing often requires data storage for lengthy periods of time, so this requirement can be a barrier for research organisations. The effort and resource required to fulfil the requirement to contact data subjects may in some cases lead to research being unviable.

    c. Article 14(5)(b) of the UK GDPR provides an exemption for controllers who process data collected indirectly from providing information to the data subjects where there would be disproportionate effort to do so. This applies to all data controllers but the Article recognises that this exemption could particularly be relevant for research purposes.

    d. Article 14(5)(b) also makes clear that the safeguards for research in article 89(1) of the UK GDPR should be a condition of this exemption, as well as appropriate measures to protect the data subject's rights, freedoms and legitimate interests, including making the information publicly available (for example, on a website). The safeguards in Section 19 of the Data Protection Act 2018 would also apply.

50. **The government is considering replicating the Article 14(5)(b) exemption in Article 13, limited only to controllers processing personal data for research purposes.** The effect of this would be to disapply the current requirement for controllers who collected personal data *directly* from the data subject to provide further information to the data subject prior to any further processing, where that further processing is for a research purpose and it would require a disproportionate effort to do so. Challenges presented by this change would include ensuring that data processing remains fair, and avoiding abuse of this provision by incentivising controllers to keep poorer records of contact details.

The government welcomes views on the following questions:

Q1.2.10. To what extent do you agree with the proposals to disapply the current requirement for controllers who collected personal data directly from the data subject to provide further information to the data subject prior to any further processing, but only where that further processing is for a research purpose and it where it would require a disproportionate effort to do so?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q1.2.11. What, if any, additional safeguards should be considered as part of this exemption?

1.3 Further Processing

51. Re-use (also known as 'further processing') of personal data can provide economic and societal benefits through facilitating innovation. Clarity on when data can lawfully be reused is important: data subjects benefit from transparency, data controllers benefit from certainty, and society benefits from unlocking the opportunities of re-use.

52. The UK GDPR states that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In recognition of the value of re-use of data in certain circumstances, the UK GDPR sets out rules for when further processing of personal data is considered compatible with the purpose for which it was collected. Article 5(1)(b) of the UK GDPR states that, subject to safeguards, further processing of personal data for scientific or historical research purposes shall ’not be considered to be incompatible with the initial purposes’.

53. The broader conditions for determining compatibility of purposes for further processing personal data are set out in Article 6(4) of the UK GDPR:

    a. Any link between the purposes for which the personal data have been collected and the purposes of the intended further processing

    b. The context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller

    c. The nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9 of the UK GDPR, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10 of the UK GDPR

    d. The possible consequences of the intended further processing for data subjects

    e. The existence of appropriate safeguards, which may include encryption or pseudonymisation

54. These conditions amount to a compatibility test for data controllers. There is a risk of uncertainty about how to interpret these rules. The government has identified three key areas of uncertainty. In each area, there may be benefits to improving clarity and thereby facilitating innovative re-use of data. However, there will also be challenges to ensure re-use remains fair and within reasonable expectations.

    a. When personal data may be re-used for a purpose different from that for which it was collected. Personal data must be collected for a specific purpose. If a controller then seeks to re-use the data for a new purpose, the UK GDPR distinguishes between purposes that are compatible with the original one and those that are incompatible. The recitals to the UK GDPR support Article 6(4) in setting out the factors to consider when determining compatible processing operations. The recitals also suggest that further processing should be permitted in some circumstances regardless of the compatibility of the purposes, and Article 6(4) seems to attempt to reflect this but its wording lacks clarity. **The government proposes to clarify that further processing for an incompatible purpose may be permitted when it safeguards an important public interest.**

    b. When personal data may be re-used by a different controller than the original controller who collected the data, and whether this constitutes further processing. Innovative data uses may involve sharing personal data sets between different controllers. Organisations seeking to process personal data for incompatible purposes, or historical, scientific, or statistical research purposes, may not be certain that they can do so lawfully if they are not the original controller. **The government is considering whether it would be useful to clarify the circumstances, if any, in which further processing can be undertaken by a controller different from the original controller, while ensuring fairness and transparency.**

    c. When further processing is taking place, and whether the original lawful ground may be relied on, when personal data is re-used. When the new purposes for processing are compatible with the original purpose, the recitals suggest that the original lawful ground for processing may still be relied on for the further processing. However, it is not always sufficiently clear what constitutes further processing and if this applies in all circumstances. For instance, when the purposes are incompatible as in section (a) above, controllers may face uncertainty about whether their new purposes constitute further processing and what their lawful ground is. **The government considers that a clarification in law may be helpful to confirm that further processing may be permitted, whether it is compatible or incompatible, when it is based on a law that safeguards an important public interest.**

The government welcomes views on the following questions:

Q1.3.1. To what extent do you agree that the provisions in Article 6(4) of the UK GDPR on further processing can cause confusion when determining what is lawful, including on the application of the elements in the compatibility test?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q1.3.2. To what extent do you agree that the government should seek to clarify in the legislative text itself that further processing may be lawful when it is a) compatible or b) incompatible but based on a law that safeguards an important public interest?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer and provide supporting evidence where possible, including on:

- *What risks and benefits you envisage*
- *What limitations or safeguards should be considered*

Q1.3.3. To what extent do you agree that the government should seek to clarify when further processing can be undertaken by a controller different from the original controller?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer and provide supporting evidence where possible, including on:

- *How you envisage clarifying when further processing can take place*
- *How you envisage clarifying the distinction between further processing and new processing*
- *What risks and benefits you envisage*
- *What limitations or safeguards should be considered*

Q1.3.4 To what extent do you agree that the government should seek to clarify when further processing may occur, when the original lawful ground was consent?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer and provide supporting evidence where possible, including on:

- *How you envisage clarifying when further processing can take place*

- *How you envisage clarifying the distinction between further processing and new processing*
- *What risks and benefits you envisage*
- *What limitations or safeguards should be considered*

1.4 Legitimate Interests

55. The UK has been a strong proponent of alternative lawful grounds to consent, recognising that there are a number of common scenarios where it may be appropriate to process personal data without seeking consent. This could be the case, for example, where it would be very difficult or inappropriate to seek the individual's consent, or where a low risk processing activity is being undertaken without consent, but in line with an individual's expectations.

56. The UK GDPR requires that all personal data processing is lawful. Therefore, data controllers must identify a lawful ground under the UK GDPR before processing personal data. These lawful grounds are set out in Article 6, which is one of the cornerstones of the UK's data protection legislation. Indeed, most data protection regimes set conditions for the legality of personal data processing. In particular, processing is permitted where:

    a. It is based on the consent of the individual

    b. It is necessary for the performance of a contract

    c. It is necessary to comply with a legal requirement

    d. It is necessary for the vital interests of an individual

    e. It is necessary for the performance of a task carried out in the public interest task or the exercise of official authority (usually by a public authority)

    f. It is necessary for the legitimate interest of a data controller where those interests are not outweighed by the data protection rights of individuals

57. Regulatory guidance in the UK is clear that no one lawful ground should be seen as always better, safer or more important than the others, and there is no hierarchy in the order of the list in the UK GDPR.[11] From engagement with stakeholders, however, the government has found that 53% of those who thought that the UK GDPR is unclear stated that they spent a disproportionate amount of time working out the requirements of the UK GDPR and the Data Protection Act 2018.[12] Further, when asked which elements of UK GDPR could be clearer, 42% identified the lawful grounds that allow data processing.[13] The government considers that this uncertainty may have resulted in an over-reliance on consent. This may lower protections for individuals, who suffer from 'consent-fatigue' in the face of a large volume of consent requests which they might accept despite not having the time or resources to assess them properly.

58. The government has heard that one factor driving over-reliance on consent is uncertainty about when it is possible to rely on the lawful ground of legitimate interests under Article 6(1)(f) of the UK GDPR. The government is also aware that some data controllers in the business sector appear to have found using legitimate interests for lawful processing to be more complicated and

[11] ICO guidance: Lawful basis for processing
[12] Ibid
[13] DCMS, 'UK Business Data Survey 2020 Summary Report', May 2021

risky than other grounds. When relying on legitimate interests as a lawful ground, the UK GDPR requires organisations to show that the processing is necessary and to document how their interests outweigh the rights of data subjects. Assessing whether the organisation's interests outweigh the rights of individuals appears to cause the most uncertainty for data controllers. This is referred to as the balancing test and the ICO has issued guidance on how to complete this test using a Legitimate Interest Assessment.

59. Ensuring appropriate use of lawful grounds is important so that organisations are empowered to use data responsibly for legitimate purposes and to provide the best outcomes to individuals. Other countries are innovating here; for example, Singapore has defined types of processing activity that would be regarded to be in the legitimate interests of the data controller, such as for investigation of proceedings, debt recovery, provision of personal and domestic services, and employment purposes. The government believes a similar approach may work well in the UK, whereby there is a definite list of processing activities that are not subject to the balancing test when relying on legitimate interests as a legal ground.

60. **The government therefore proposes to create a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test in order to give them more confidence to process personal data without unnecessary recourse to consent.** The processing would still have to be necessary for the stated purposes and proportionate. For those activities not on the list, the balancing test would still be applied. The balancing test could also be maintained for use of children's data, irrespective of whether the data was being processed in connection with an activity on the list. The government is mindful that Article 6(1)(f) of the UK GDPR recognises that particular care should be taken when data controllers are relying on the legitimate interests lawful ground to process data relating to children.

61. Any list would also need to be sufficiently generic to withstand the test of time, although the government envisages it could be updated via a regulation-making power. In that respect, the list would be similar to the approach in Section 8 of the Data Protection Act 2018 for the public tasks processing condition. For example, it could cover processing activities which are necessary for:

    a. Reporting of criminal acts or safeguarding concerns to appropriate authorities

    b. Delivering statutory public communications and public health and safety messages by non-public bodies

    c. Monitoring, detecting or correcting bias in relation to developing AI systems (see section 1.5 for further details)

    d. Using audience measurement cookies or similar technologies to improve web pages that are frequently visited by service users

    e. Improving or reviewing an organisation's system or network security

    f. Improving the safety of a product or service that the organisation provides or delivers

    g. De-identifying personal data through pseudonymisation or anonymisation to to improve data security

    h. Using personal data for internal research and development purposes, or business innovation purposes aimed at improving services for customers

i. Managing or maintaining a database to ensure that records of individuals are accurate and up to date, and to avoid unnecessary duplication

62. The government considers this approach could create a better balance between protecting individuals and not impeding responsible data use in these specific circumstances. Broader data protection principles and safeguards would also continue to apply where appropriate, including safeguards in relation to the processing of any sensitive data and data relating to children.

The government welcomes views on the following questions:

Q1.4.1. To what extent do you agree with the proposal to create a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q1.4.2. To what extent do you agree with the suggested list of activities where the legitimate interests balancing test would not be required?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, indicating whether and why you would remove any activities listed above or add further activities to this list.

Q1.4.3. What, if any, additional safeguards do you think would need to be put in place?

Q1.4.4. To what extent do you agree that the legitimate interests balancing test should be maintained for children's data, irrespective of whether the data is being processed for one of the listed activities?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

1.5 AI and Machine Learning

63. Used responsibly, data-driven artificial intelligence (AI) systems have the potential to bring incredible benefits to our lives.

Case study: *Using AI technology to improve patient care*
Researchers from Moorfields Eye Hospital and the University College London Institute of Ophthalmology recently made a breakthrough in patient care using AI technology. The researchers successfully trained machine learning technology on thousands of historic de-personalised eye scans to identify signs of eye disease and recommend how patients should be referred for care. This AI system can recommend the correct referral decision for over 50 eye diseases with 94% accuracy, matching world-leading eye experts. This innovation has the potential to revolutionise the way that professionals carry out eye tests, allowing them to spot conditions earlier and prioritise patients with the most serious eye diseases before irreversible damage sets in.

64. The development of AI and machine learning applications is contingent on data, and places specific demands on its collection, curation and use. A National AI Strategy will be published later this year to set out how the government plans to build on the UK's leadership in AI. Whereas the National AI Strategy will address a wide range of issues arising from the emergence of AI technologies, this consultation focuses on the interplay of AI technologies with the UK's data protection regime.

65. The right reforms to the UK's data protection framework can help organisations building or deploying AI tools to innovate responsibly, manage data-related risks at every stage of the AI lifecycle, and ensure that individuals can trust that their personal data is used responsibly. Reforms should aim to help organisations building or deploying AI tools to interpret existing data regulation. Reforms should also simplify legislation, where appropriate, so potential new entrants to data-driven markets are not deterred and beneficial, responsible data use is not impeded.

66. There are multiple, sometimes conflicting, definitions of artificial intelligence. For the purpose of this document, the following terminology is in use:

    a. Artificial intelligence: the use of digital technology to create systems capable of performing tasks commonly thought to require intelligence. AI is constantly evolving, but generally it involves machines using statistics to find patterns in large amounts of data, and the ability to perform repetitive tasks with data without the need for constant human guidance[14]

    b. Machine learning: a subset of AI referring to the development of digital systems that improve their performance on a given task over time through experience. Machine

[14] Government Digital Service, Office for Artificial Intelligence , 'A guide to using artificial intelligence in the public sector', 2019

learning is the most widely-used form of AI, and has contributed to innovations like self-driving cars, speech recognition and machine translation[15]

c. Automated decision-making: the process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data.[16] Automated decision-making processes often make use of AI/machine learning, but not always

d. Profiling: any form of automated processing of personal data consisting of the use of personal data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements[17]

e. Bias: an unfair skew based on characteristics, arbitrary factors, or an otherwise inappropriate basis

Explanatory box: *Data in an AI lifecycle*

Data (both personal and non-personal data) features in every stage of a typical AI lifecycle. We briefly describe how this works in the context of an example of an AI-automated decision-making process; it is important to note that this is an ongoing and iterative process.

- A set of data (personal and non-personal) is gathered; for example, a collection of input data from historical applications for a service (e.g. a loan) along with the decisions reached and any data on whether those outcomes were the right ones (e.g. whether the loan repaid)
- Then, a machine-learning algorithm is chosen and uses historical data (e.g. a set of past input data, the decisions reached) to build a model, optimising against a set of criteria specified by a human
- The resulting model is then used repeatedly as part of the decision-making process, either to make an automated decision, or to offer guidance to a human making the final decision
- New input data and associated decisions can be fed back into the data set to enable the model to be updated (either periodically or continuously)
- The above learning process feeds on data, the machine learning algorithm and the machine learning model[18]

Data enters this lifecycle in 4 places:

[15] Ibid.
[16] ICO Guidance: 'What is automated individual decision-making and profiling?'
[17] Current UK GDPR definition; UK GDPR Article 4(4).
[18] This is an indicative process only for the purposes of this consultation document; there are many variations to this process.

- **Training data:** The large set of data used for the purpose of training a model (not to directly make decisions about individuals in that training set)
- **Input data:** The data available about a person (e.g. an applicant for a service) that will serve as a basis for the decision about that individual
- **Outcome(s) data:** Data describing the outcomes of decisions (i.e. measuring average outcomes of a decision-making process and assessing how they compare to an expected baseline)
- **Baseline data:** In some cases, meaningfully assessing data on outcomes requires access to appropriate data to compare the outcome to (e.g. what rates of acceptance of different groups might be expected in a fair process)

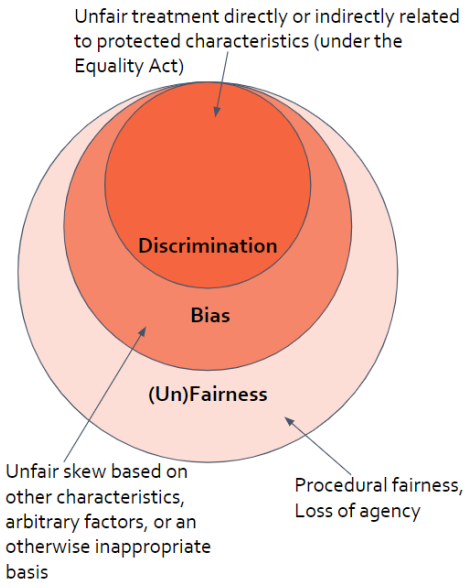
67. The UK GDPR is technology-neutral and was not intended to govern AI systems comprehensively, nor any other specific technologies. Many AI systems also do not use personal data at all. Currently, the UK data protection framework (UK GDPR and Data Protection Act 2018) draws no specific distinction between the different uses of data within an AI process - except to the extent that the UK GDPR does distinguish between research purposes (which may include AI research) and non-research purposes - and applies the same rules to all stages where personal data enters the AI lifecycle even though there may be material differences between them. The ICO's Guidance on AI and Data Protection, however, recognises that differentiation is necessary: *"In many cases, when determining your purpose(s) and lawful basis, it will make sense for you to separate the research and development phase (including conceptualisation, design, training and model selection) of AI systems from the deployment phase. This is because these are distinct and separate purposes, with different circumstances and risks."* The UK GDPR does contain specific provisions on automated decision-making, including profiling (Article 22). Overall, navigating and applying relevant data protection provisions is a complex exercise for an organisation looking to develop or deploy AI tools, possibly impeding their uptake, or generating confusion.

68. The government recognises that the governance of AI technologies is a live debate. Regulatory oversight, support and guidance will remain important as these technologies develop rapidly. The overarching legal framework should remain fit for purpose as technology, including AI tools, changes the world around us. This temperature check is important: it has been almost five years since the UK GDPR was first drafted, and three years since its adoption. The government intends to retain the technology-neutral design of the UK GDPR and to ensure that the legal framework is not at risk of permitting technology-driven harms, or of unduly impeding data-driven innovation.

Fairness in an AI context

69. The government expects AI systems and their use to be fair. In order to reap the many benefits that responsible AI can deliver, algorithms must be developed and deployed fairly. Fairness is particularly important as breakthroughs in in the fields of AI and data science create novel risks

by potentially amplifying existing biases and discrimination in data, enhancing existing inequality, or increasing vulnerability to malfunction or manipulation.



70. Fairness is necessarily broad and context-specific, and many different concepts of fairness exist. There are many definitions of fairness, which are not all consistent with each other, reflecting differing contexts, opinions and priorities. Fairness can be defined by multiple parameters, ranging from mathematical or technical requirements that relate to outputs, to social or sociological requirements that relate to a fair process. Expectations and legal requirements on fairness currently vary widely. There is a close nexus between fairness, bias, and discrimination, and for the purpose of this consultation, we are treating anti-discrimination, equality measures and measures to combat bias as within the wider ambit of fairness.[19]

71. In legal terms, concepts of fairness exist in several legislative frameworks, also outside of data protection. This includes concepts of 'fair data use', 'fairness of process', as well as 'fairness of outcomes' that are drawn, for example, from consumer protection, employment, equality, and human rights law. The table below presents an illustrative and non-exhaustive mapping.

Concept	Description	Current legislation
Fair data use	• Using personal data as people expect you to use it, and being open about how data will be used	• UK GDPR principle of Article 5(1)(a) that data should be processed lawfully, fairly and in a transparent manner • Ex ante (before the fact) 'fair balancing' mechanisms: the conditions for lawful processing in Article 6(1) UK GDPR (e.g. consent (Article 6(1)(a)), contract (Article 6(1)(b)) and legitimate interest (Article 6(1)(f)) • Ex post (after the fact) fairness mechanisms: key data subject rights such as UK GDPR Article 16 - Right to Rectification and UK GDPR Article 21 - the right to object to data processing carried out under a legal basis consent.

[19] Similar to the approach taken in the Centre for Data Ethics and Innovaton's 'Review into bias in algorithmic decision-making', 27 Nov 2020.

Concept	Description	Current legislation
Procedural fairness	● Following a fair procedure or process when making a decision, defining an objective set of criteria for decisions, and enabling individuals to understand and challenge decisions about them	Aspects of this are covered in various laws, including: ● UK GDPR Article 22: Data subjects have a right to not be subject to a solely automated decision-making process with significant effects ● UK GDPR Article 15 ('Right of Access') ● UK GDPR Article 21 ('Right to Object') ● Administrative law - administrative decision makers need to come to a decision in a procedurally 'fair' way- otherwise, the decision may be unlawful; administrative decision makers must avoid bias in making decisions ● Aspects of Equality Act 2010 e.g. reasonable adjustments for disability, Public Sector Equality Duty ● European Convention on Human Rights - Article 6 - right to a fair trial (as given further effect in UK law through the Human Rights Act 1998) ● Competition & Markets legislation; fair process for consumers, fair terms in contracts ● Sectoral regulations, such as for financial services ● The prohibition on unfair contract terms under the Consumer Rights Act 2015
Outcome fairness	● Fair outcomes of decisions, e.g. equal outcomes for different demographic groups ● There is a large array of different definitions of outcome fairness, many of which are mutually	● Equality Act 2010 *e.g. Direct & Indirect Discrimination* ● European Convention on Human Rights Article 14 - prohibition of discrimination (as given further effect in UK law through the Human Rights Act 1998), in conjunction with substantive Convention rights

Concept	Description	Current legislation
	incompatible. A growing set of academic literature and technical tools in this area provide an array of options for practitioners, but less clarity on which approaches are appropriate when	• UK GDPR Recital 71 advises that organisations should avoid any form of profiling that results in "discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or processing that results in measures having such an effect" • Employer's duties not to unfairly dismiss under the Employment Rights Act 1996

72. Navigating and applying concepts of fairness in the context of AI systems is a complex exercise for two reasons:

    a. Limited understanding of how to apply 'fairness': on the one hand, there is too little specific guidance for practitioners to apply the concept of fairness to building and using trustworthy AI systems. This was demonstrated in the Centre for Data Ethics and Innovation's Review into Bias in Algorithmic Decision-making, which found that organisations do not always understand their responsibilities under the Equality Act when using algorithmic decision-making, and that there is insufficient legal clarity concerning novel bias mitigation techniques

    b. Surfeit of guidance: on the other hand, the current AI governance landscape is fragmented, with a plethora of actors producing guidelines and frameworks to help fill gaps in organisations' understanding. This includes regulators - the ICO and the Equality and Human Rights Commission, as well as relevant sector regulators such as the Financial Conduct Authority and the Competition & Markets Authority - and also includes non-regulatory actors such as the Centre for Data Ethics & Innovation, the Ada Lovelace Institute, the Open Data Institute, and the Alan Turing Institute. International organisations have also started to develop frameworks; for example, the OECD AI Principles, UNESCO's Recommendation on the ethics of artificial intelligence, and the Ad hoc Committee on Artificial Intelligence of the Council of Europe's consultation on a legal framework for AI. This proliferation of initiatives, alongside the existing complexity of applying fairness due to its context-specific nature, risks creating uncertainty on which standards or processes organisations looking to develop and deploy AI systems fairly should follow

73. The operation of the concept of 'fairness' in data protection regulation may also contribute to this uncertainty. Fairness is a widely recognised concept and is present in a significant number of data protection laws. The requirement for 'fair' processing forms part of the 'lawfulness, fairness and transparency' principle under the UK GDPR, which states: *"[Personal data shall be] processed lawfully, fairly and in a transparent manner in relation to the data subject"* (Article 5(1)(a)). Recital 39 of the UK GDPR offers some further explanation of what constitutes

transparent processing, but does not provide any explicit detail on what is specifically meant by fair processing.

74. In the context of data protection, the concept of fairness was originally understood as akin to transparency. There is a close connection between fairness and transparency because, in part, 'fairness' currently relates to the understanding or expectations of the data subject – and in accordance with the transparency principle, a controller must tell data subjects how and why it will process their personal data. If a controller processes personal data in a way that is unjust or unexpected, such processing is inherently unfair. The ICO has stipulated in guidance that a controller should 'only handle personal data in ways that people would reasonably expect' and, crucially, 'not use it in ways that have unjustified adverse effects on them'.[20] The latter is broader than transparency requirements alone.

75. Big data analysis, predictive analytics and AI applications are examples of data processing in relation to which many data subjects do not have clear expectations or understanding. This presents clear challenges to the transparency of data processing for individuals. Such data processing activities have the potential for significant adverse effects, and campaign groups, as well as members of the public more broadly, have voiced concerns about the fairness of such technologies.

76. The ICO, as part of its Guidance to AI and Data Protection, has elaborated on the concept of fairness in an AI context. In addition to the general fairness requirements, the ICO interprets that fair data processing involves 'ensuring an AI system is statistically accurate; avoiding discrimination in the use of AI for decision-making; the possibility of making incorrect inferences about people using AI; and the consequences of false positives versus false negatives [are considered]'.[21]

77. Understanding of fair data processing has begun to move beyond transparency requirements. The ICO's guidance suggests that the fairness principle is potnetially quite expansive, stating that 'any processing of personal data using AI that leads to unjust discrimination between people, will violate the fairness principle'.[22] However, the ICO recognises the primacy of other laws and authorities to determine substantive aspects of fairness in the same guidance: '[the ICO] do[es] not aim to provide guidance on legal compliance with the UK's anti-discrimination legal framework, notably the UK Equality Act 2010'.[23] In practice, the ICO has also not to date taken enforcement action except in relation to fair data use and procedural fairness.

78. The government is concerned that there is uncertainty about the scope and substance of 'fairness' in the data protection regime as applied to the development and deployment of AI systems, and the ICO's regulatory reach. There is a risk of regulatory confusion for organisations because the current legislative framework could allow a very broad interpretation of fairness (fair data use, fairness of process, and outcome fairness) in the context of data protection as applied to AI systems. If concepts of fairness as defined by the ICO, the Equality and Human Rights Commission, the Competition and Markets Authority, and others all apply in overlapping ways to an AI use case then it may well be unclear to organisations how to assess whether AI use is fair.

79. Comprehensively defining 'outcome fairness' in the context of AI within the data protection regime may therefore not be a feasible or effective approach. The government assesses that

[20] ICO Guidance: Principle (a): Lawfulness, fairness and transparency
[21] ICO Guidance: What do we need to do to ensure lawfulness, fairness, and transparency in AI systems?
[22] ICO Guidance: AI and Data Protection
[23] Ibid.

other horizontal or sectoral laws and associated regulators may provide a more appropriate avenue for the assessment of some aspects of fairness, especially of fair outcomes, in the context of AI systems. The UK's AI governance framework should provide clarity about an organisation's responsibilities with regards to fair data use, procedural fairness, and outcome fairness when applied to developing and deploying an AI system. The government also wants to ensure that the right regulatory responsibility and capability is in place.

80. Navigating the concept of fairness poses important questions for the future of AI governance. This is important both to ensure that the future AI regime protects people and works for society as a whole, and to create regulatory clarity so that organisations need not navigate a wide range of fairness provisions, which may confuse the responsible development of AI tools. The National AI Strategy to be published later this year will address these areas in more depth.

The government welcomes views on the following questions:

Q1.5.1. To what extent do you agree that the current legal obligations with regards to fairness are clear when developing or deploying an AI system?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q1.5.2. To what extent do you agree that the application of the concept of fairness within the data protection regime in relation to AI systems is currently unclear?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible

Q1.5.3. What legislative regimes and associated regulators should play a role in substantive assessments of fairness, especially of outcomes, in the AI context?

Please explain your response.

Q1.5.4. To what extent do you 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?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*

- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible, including on the risks.

Building trustworthy AI systems

81. The use of algorithmic, or automated decision-making is likely to increase substantially in coming years. Organisations should be confident that their AI-powered services are a force for good and will not inadvertently harm consumers. They need the right tools to build trustworthy and fair AI systems.

82. To that end, the government recognises that organisations developing and deploying AI tools responsibly would benefit from the freedom to experiment where it does not cause harm. The government is considering how to develop a safe regulatory space for the responsible development, testing and training of AI.

83. The market is still in the early stages of navigating UK GDPR provisions for the purposes of developing and deploying AI systems, and it is therefore difficult to pin down one particular compliance challenge. Rather, there is general uncertainty among those looking to deploy AI-related tools, or to use personal data to help train system development, about how that activity fits within the current regulatory environment. Currently, an AI practitioner needs to consider each use case individually and work out each time whether the data protection regime permits the activities. This creates doubt and uncertainty which may lead to friction and a potential reduction in innovation.

84. There are existing initiatives, such as the ICO Regulatory Sandbox, that enable innovators to test and trial ideas under enhanced supervision by the regulator. In addition to these initiatives, and subject to appropriate safeguards, the government is considering how to permit organisations to use personal data more freely, such as for the purpose of training and testing AI responsibly, in line with the OECD Principles on Artificial Intelligence. This means ensuring such use is appropriately fair, accountable, transparent, secure and ultimately trustworthy. The government recognises the challenges with applying these high-level principles to contexts such as AI training and testing. The Central Digital and Data Office's Data Ethics Framework and the work of the Centre for Data Ethics and Innovation provide guidance on delivering responsible innovation.

The government welcomes views on the following questions:

Q1.5.5. To what extent do you agree that the government should permit organisations to use personal data more freely, subject to appropriate safeguards, for the purpose of training and testing AI responsibly?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible, including which safeguards should be in place.

Q1.5.6. When developing and deploying AI, do you experience issues with identifying an initial lawful ground?

Please explain your answer, and provide supporting evidence where possible.

Q1.5.7 When developing and deploying AI, do you experience issues with navigating re-use limitations in the current framework?

Please explain your answer, and provide supporting evidence where possible.

Q1.5.8 When developing and deploying AI, do you experience issues with navigating relevant research provisions?

Please explain your answer, and provide supporting evidence where possible.

Q1.5.9 When developing and deploying AI, do you experience issues in other areas that are not covered by the questions immediately above?

Please explain your answer, and provide supporting evidence where possible.

85. Monitoring, detecting and correcting bias is an important aspect of algorithmic testing and training, and critical to ensuring an AI system works appropriately and fairly. The Centre for Data Ethics and Innovation's AI Barometer report found that bias in algorithmic decisions was seen as the biggest risk arising from the use of data-driven technology across all sectors examined (Criminal Justice, Financial Services, Health and Social Care, Digital and Social Media, Energy and Utilities). As one example, it was found that to mitigate this risk, financial services firms should take steps to prevent their algorithmic systems from replicating societal and historic discrimination (e.g. red lining poorer neighbourhoods within the insurance industry). Financial firms should also be aware of the inferences they can now draw about customers using AI, some of which could be deemed unfair (e.g. insurers predicting someone's fitness levels from their purchasing habits).

86. Good use of data can enable organisations to shine a light on existing practices and identify what is driving bias. Data is needed to monitor outcomes and identify and mitigate bias, but it is not widely understood how personal data, and sensitive personal data, can be processed for that purpose. The Centre for Data Ethics and Innovation's Review into Bias in Algorithmic Decision-making found that a lack of common understanding on this issue is paralysing for organisations, directly impacting the representativeness and quality of algorithms and their services, including in the public sector.

Case study: *Challenges to demographic data collection and use in pursuit of fairness*

The Partnership on AI conducted a study on the way that demographic data collection and use proceeds in practice.[24] The study found that perceived legal barriers to accessing demographic data make it difficult to take action to address algorithmic bias. Almost every participant described access to demographic data as a significant barrier to implementing various technical fairness techniques. Outside of employment, healthcare, and the occasional financial service contexts, few practitioners had direct access to data on race, so most did not try to assess their systems and products for racial bias.

Although the Partnership on AI is US-based, this study demonstrated the reach of UK GDPR regulation, and the findings indicate a more universal problem. These findings are supported by the Centre for Data Ethics and Innovation's Review into Bias in Algorithmic Decision-making which found that there were widespread perceptions that data protection is a barrier to collecting and processing demographic data.[25]

87. The ICO, in its Guidance on AI and Data Protection, also recognises that it may be necessary to use personal data, including sensitive personal data, for bias detection and mitigation purposes. Despite this recognition, the steps to use personal data and sensitive personal data for this purpose can be perceived as onerous. In some circumstances it may be necessary to obtain explicit consent from an individual to use their sensitive personal data to monitor or mitigate bias. Making explicit that consent is a prerequisite for data access may in itself risk introducing bias into the data used in an AI system, as in practice, every time an individual refuses to provide consent to processing, a dataset may become unrepresentative. As a consequence, any output of the AI application may be biased towards the demographic of individuals willing to consent to processing.

Explanatory box: *The need to use demographic data to detect and mitigate bias*

Given the known risk that automated decision-making processes can be biased, it is often appropriate to use data to attempt to measure potential biases, and guide assessments of how processes are biased, and what could be done to address this.

In its simplest form, bias detection often involves collection of demographic data (e.g. data on the sex and race of those that decisions are being made about), and then making a statistical assessment of any disparities. There are various different approaches to this reflecting different possible notions of what a fair outcome might look like, for example:

[24]McKane Andrus, Elena Spitzer, Jeffrey Brown, and Alice Xiang. 2021. "What We Can't Measure, We Can't Understand": Challenges to Demographic Data Procurement in the Pursuit of Fairness. In Conference on Fairness, Accountability, and Transparency (FAccT '21), March 3–10, 2021, Virtual Event, Canada.
[25]Centre for Data Ethics and Innovation, Review into bias in algorithmic decision-making, November 2020. pp. 89-93.

- **Demographic Parity** - outcomes for different protected groups are equally distributed, and statistically independent

- **Conditional Demographic Parity** - as above, but "legitimate risk factors" might mean that we consider it fair to discriminate for certain groups, such as by age in car insurance. The difficulty then sits in deciding which factors qualify as legitimate, and which may be perpetuating historical biases

- **Equalised Odds (separation)** - qualified and unqualified candidates are treated the same, regardless of their protected attributes. True positive rates are the same for all protected groups, as are false positive rates: the chance that a qualified individual is overlooked, or that an unqualified individual is approved, is the same across all protected groups

- **Calibration** - outcomes for each protected group are predicted with equal reliability

Where bias is detected within a model, there are a variety of 'bias mitigation techniques' available to machine learning practitioners, also typically drawing on demographic data.

88. In the current data protection legislative framework, the lawful grounds for processing personal data in the UK GDPR (Article 6) and for special category and criminal convictions data (Articles 9 and 10) do not explicitly permit the processing of personal data or sensitive personal data to monitor, detect and correct algorithmic bias.

89. Whilst recognising that data protection legislation is far from the only means by which to address algorithmic fairness, there are actions that can be taken within this reform agenda to protect people from algorithmic discrimination and to simplify the data protection rules in order to perform bias mitigation interventions. The government wants to enable organisations to use personal data and sensitive personal data for the purpose of managing the risk of bias in their AI systems and, to address this, the government is inviting views on the following proposals.

90. As detailed in section 1.4, the government proposes creating a limited, exhaustive list of legitimate interests for which businesses can use personal data without applying the balancing test, thereby giving organisations more confidence to process personal data without unnecessary recourse to consent. The processing would still have to be necessary and proportionate. **The government proposes to stipulate in this list that processing personal data for the purposes of ensuring bias monitoring, detection and correction in relation to AI systems constitutes a legitimate interest in the terms of Article 6(1)(f) for which the balancing test is not required.**

91. **Where bias monitoring, detection or correction can only be undertaken with the use of sensitive personal data, the government proposes to either:**

    a. **Make it clear that the existing derogation in Paragraph 8 of Schedule 1 to the Data Protection Act 2018 can be used for this type of processing.** This Paragraph addresses processing of sensitive personal data necessary 'for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment of [specified vulnerable] people'. Whilst data protection principles would also still apply, utilising this derogation could provide a basic gateway to support algorithmic bias

monitoring involving special category data. This could be explained with further AI-focused guidance by the regulator which would assist data controllers to identify which Schedule 1 processing condition is relevant; or

b. **Create a new condition within Schedule 1 to the Data Protection Act 2018 which specifically addresses the processing of sensitive personal data as necessary for bias monitoring, detection and correction in relation to AI systems.** This approach would (i) create certainty on how and when bias monitoring is permitted; (ii) make a clear reference to AI as a supported technology within the Data Protection Act 2018 framework; and (iii) give a clear direction that the derogation is of general application where necessary and appropriate to support AI system development in general. For the condition to be effective, it would be necessary to clarify the parameters for its use, and should include specific requirements. These could include: (i) ensuring the processing is strictly necessary for this purpose; (ii) data is explicitly collected for bias/discrimination mitigation and not for any other purpose; and (iii) appropriate safeguards to remove risks of secondary use, e.g. by specifying technical limitations on re-use, and the implementation of appropriate security and privacy preserving measures. Attributes and safeguarding parameters such as these may enhance public trust that data collected for this purpose is for a broader public benefit, and would additionally instil confidence in AI practitioners to process the necessary data for this purpose.

92. The government is aware that the proposal at paragraph 91 b may result in a disproportionate increase of processing of personal data of individuals with protected characteristics. The more an individual's personal data is processed, the greater the likelihood of intrusion into their private and family life, and the greater the risk of a breach involving their personal data. Generally, a provision that will result in more processing could be characterised as adverse for affected individuals. However, the purpose of this proposal is to support organisations to monitor harmful bias and eliminate discrimination, so any detrimental impact is considered objectively justifiable. Furthermore, the more representative the data that an AI system is trained on, the more the system will reflect a broader cross-section of the population. This in itself is likely to mitigate bias and discrimination, and the government assesses that unjustified discriminatory AI systems are likely to generate greater adverse impacts on an individual with protected characteristics than the potential for a data breach or a greater level of intrusion.

The government welcomes views on the following questions:

Q1.5.10. To what extent do you agree with the proposal to make it explicit that the processing of personal data for the purpose of bias monitoring, detection and correction in relation to AI systems should be part of a limited, exhaustive list of legitimate interests that organisations can use personal data for without applying the balancing test?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible, including on:

- *the key benefits or risks you envisage*

- *what you envisage the parameters of the processing activity should be*

Q1.5.11. To what extent do you agree that further legal clarity is needed on how sensitive personal data can be lawfully processed for the purpose of ensuring bias monitoring, detection and correction in relation to AI systems?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q1.5.12. To what extent do you agree with the proposal to create a new condition within Schedule 1 to the Data Protection Act 2018 to support the processing of sensitive personal data for the purpose of bias monitoring, detection and correction in relation to AI systems?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q1.5.13 What additional safeguards do you think would need to be put in place?

93. Of course, stakeholders should consider complementary approaches to tackling bias and discrimination, such as the mitigation of risks at the design stage, the environment in which AI systems are deployed, or the use of independent data intermediaries (see section 1.7). The government's proposals within this reform agenda should be seen as part of a holistic framework that needs to be set in place, and which will be considered and further set out through the National AI Strategy.

Automated decision-making and data rights

94. Taking a holistic view of the development and deployment of AI systems is pivotal in addressing the risks in AI-powered automated decision-making and in deciding the controls required to build and maintain trust in their application. The trustworthiness of the systems will hinge on specific design features, as outlined above, but also on effective safeguards where needed (e.g. human oversight at key points to ensure clear traceability of accountability) and the intelligibility (not merely 'explainability') of decisions taken.

95. Decision-making processes that rely on AI technologies are one aspect of this holistic view. Article 22 in the UK GDPR contains specific provisions on automated individual decision-making

and profiling.[26] It is important to note that not all AI systems automatically trigger the application of Article 22; the rules are intended to protect individuals in the context of 'solely automated' decision-making that 'produces legal effects concerning him or her or similarly significantly affects him or her'. An organisation must identify whether any of the processing falls under Article 22 and, if so, is required to: (i) give individuals specific information about the processing; (ii) take steps to prevent errors, bias and discrimination; and (iii) give individuals rights to challenge and request a review of the decision ('right to human review').[27]

Case Study: *Impact of Article 22 on Vaccine Prioritisation*

QCOVID is a predictive risk model that was developed to support decisions on vaccine prioritisation. It operates by inputting individuals' personal health data into a tool, which uses an algorithm to identify those individuals at highest risk of serious adverse consequences as a result of catching COVID-19. Once these individuals were identified by the tool they were automatically prioritised for vaccination and added to the Shielded Patient List. The model identified approximately 1.5 million people who were added to the Shielded Patient List and offered vaccine prioritisation.

Article 22(1) of UK GDPR required the NHS to consider whether adoption of the QCOVID algorithm to help with vaccine prioritisation involved taking an automated decision that had 'legal effects' or 'similarly significant effects' on individuals on a 'solely automated' basis (i.e. without human involvement).

A key question was whether the level of GP involvement in the decision making process comprised sufficient human intervention to mean that this was not a solely automated decision. It was determined that GPs were able to meaningfully review the decision to add patients to the Shielded Patient List, constituting sufficient human intervention. The NHS reminded GPs (in guidance letters sent by DHSC) that it was important to review the Shielded Patient List based on their clinical knowledge of the patient.

96. The government recognises that the safeguards under Article 22 are meaningful in some use cases, especially as there is currently no clear consensus on approaches and standards for wider AI governance. There might be a legitimate need for certain 'high risk' AI-derived decisions to require a human review, even if this restricts the scope of use of such systems or makes them slower.

97. However, the current operation and efficacy of Article 22 is subject to uncertainty, as set out below.

    a. **Lack of certainty on how and when current safeguards are intended to apply in practice.** Provisions in the UK GDPR for explainability and transparency in relation to algorithms are restricted to those decisions that are based 'solely on automated processing' (and therefore captured by Article 22). In reality, most automated decisions have a human involved at some point, even if their involvement is superficial or

[26] 'Any form of automated processing of personal data consisting of the use of personal data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour location or movements', UK GDPR Article 4.

[27] ICO, Guide to General Data Protection Regulation (GDPR) - Rights related to automated decision making including profiling

substantially biased by the verdict of the algorithm, or their own judgement is affected by other conscious or unconscious biases. When transparency provisions are triggered, there is a requirement that the data controller provides 'meaningful information about the logic involved, as well as the significance and envisaged consequences of processing for the data subject' - but it is not well established what this means.[28]

For example, the Centre for Data Ethics and Innovation considered the use of algorithmic tools in recruitment, and the specific use case of 'solely' automated rejections for candidates at the application stage. It was found that organisations did not have clarity about how to make arrangements for 'the right to human review' when applied to screening thousands of candidates. Indeed, it was found that the guidance is rarely applied in the way outlined by the ICO, and in particular with respect to introducing ways to request human intervention or review when carrying out large scale sifts by either algorithmic or non-algorithmic methods.[29]

Further terminology ('similarly significant effects') may sometimes lead organisations to assume that the Article does not apply to them or their processing activities, potentially foregoing the safeguards where they are needed, or reverting to a risk-averse approach as a default resulting in not automating decisions at all.

b. **Limited application of the Article.** As a result of the current terminology, a lot of profiling and AI-related processing activity will likely fall outside of the Article 22 regime - for example, when carrying out a partly (but not 'solely') automated decision, or when an automated decision is taken based on 'non-personal' data. As a result, automated decisions with a 'legal or similarly significant effect' might not be subject to safeguards (when they might be needed), and the safeguards as introduced for 'solely automated' decisions may be disproportionate, or unduly circumvented (e.g. by introducing token human oversight so as not to be captured as 'solely automated'). Obviously the UK's data protection regime alone cannot be the right vehicle to address these limitations fully, especially in relation to decisions driven by non-personal data.

   As currently framed, Article 22 provides for the data subject to have the right not to be subject to a decision that has either legal or 'similarly significant' effects based solely on automated processing, including profiling, unless an exception applies.[30] This can be considered too restrictive to ensure that the UK GDPR remains principle-based and future-proofed in light of evolving machine learning and AI technologies. This is further complicated by the fact that what constitutes a legal or 'similarly significant' effect produced by an automated decision under Article 22 of the UK GDPR is open to interpretation.

98. The above issues need to be viewed in the context that the use of automated decision making is likely to increase greatly in many industries in the coming years. The need to maintain a capability to provide human review may, in future, not be practicable or proportionate, and it is important to assess when this safeguard is needed and how it works in practice.

99. It is critical that UK GDPR's provisions for automated decision-making and profiling work for organisations and for individuals. It is therefore important to examine whether Article 22 and its

[28] Article 13 2(f) UK GDPR, and Article 14 2(g) UK GDPR.
[29] CDEI Review into bias in algorithmic decision-making, p. 47.
[30] See exceptions detailed at Article 22(2) of the UK GDPR

provisions are keeping pace with the likely evolution of a data-driven economy and society, and whether it provides the necessary protection.

100. There is limited case law to clarify how Article 22 in the UK GDPR works in practice, or indeed how the UK GDPR is interpreted in specific AI contexts. The evidence on how practitioners interact with Article 22 is slim. As such, the government is seeking further evidence on the potential need for legislative reform rather than making proposals at this stage. Responses to this consultation will help build an evidence base on this relatively new provision and its efficacy to inform our future policy approach.

The government welcomes views on the following questions:

Q1.5.14. To what extent do you agree with what the government is considering in relation to clarifying the limits and scope of what constitutes 'a decision based solely on automated processing' and 'produc[ing] legal effects concerning [a person] or similarly significant effects?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible, including on:

- *The benefits and risks of clarifying the limits and scope of 'solely automated processing'*
- *The benefits and risks of clarifying the limits and scope of 'similarly significant effects'*

Q1.5.15. Are there any alternatives you would consider to address the problem?

- *Yes*
- *No*
- *Don't know*

Please explain your answer, and provide supporting evidence where possible.

Q1.5.16. To what extent do you agree with the following statement: 'In the expectation of more widespread adoption of automated decision-making, Article 22 is (i) sufficiently future-proofed, so as to be practical and proportionate, whilst (ii) retaining meaningful safeguards'?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible, on both elements of this question, providing suggestions for change where relevant.

101. The Taskforce on Innovation, Growth and Regulatory Reform has recommended that Article 22 of UK GDPR should be removed. The report recommends that UK law should instead permit the use of solely automated AI systems on the basis of legitimate interests or public interests. Such a change would remove the right not to be subject to a decision resulting from 'solely automated' processing if that decision has legal or 'similarly significant' effects on data subjects. This would mean that solely automated decision-making in relation to personal data would be permitted, subject to it meeting other requirements of the data protection legislation, including the conditions of lawful processing in Article 6(1) of the UK GDPR (and, Articles 9 and 10, as supplemented by Schedule 1 to the Data Protection Act 2018) in relation to sensitive personal data, where relevant. The government is considering this proposal and is seeking views from stakeholders.

The government welcomes views on the following questions:

Q1.5.17. To what extent do you agree with the Taskforce on Innovation, Growth and Regulatory Reform's recommendation that Article 22 of UK GDPR should be removed and solely automated decision making permitted where it meets a lawful ground in Article 6(1) (and Article 9-10 (as supplemented by Schedule 1 to the Data Protection Act 2018) where relevant) and subject to compliance with the rest of the data protection legislation?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible, including on:

- *The benefits and risks of the Taskforce's proposal to remove Article 22 and permit solely automated decision making where (i) it meets a lawful ground in Article 6(1) (and, Articles 9 and 10, as supplemented by Schedule 1 to the Data Protection Act 2018) in relation to sensitive personal data, where relevant) and subject to compliance with the rest of the data protection legislation.*

- *Any additional safeguards that should be in place for solely automated processing of personal data, given that removal of Article 22 would remove the safeguards currently listed in Article 22 (3) and (4)*

Public trust in the use of data-driven systems

102. The collective analysis and sorting of an individual's personal data into groups by algorithms means that people can be impacted by other people's data in aggregate (or collectively), as well as by data about themselves. In many business models, commercial value lies in the inferences drawn from an individual's behaviour, and the 'profile' that is construed by the combination of those personal data points. Inferences made by an AI system could have significant consequences, for instance on an individual's prospects of getting a job. Given inferences are often made based on ad hoc group-level characteristics (e.g. based on groupings of certain types of behaviour), there is a risk of bias in decisions made about individuals based on their

membership of an algorithmically defined group. Additionally, analysis of biometric and physiological data can reveal highly sensitive attributes about a person, but without necessarily identifying them. This so-called 'soft biometric data' may then be used in a way that significantly impacts an algorithmically defined group, without identifying specific individuals within that group. Individuals may have limited visibility or knowledge of the inferences organisations may draw about them and the categories in which they are placed. Various academics and commentators have argued that additional safeguards are required to protect against such group level bias that does not align directly with protected characteristics.[31]

103. The government wants the application of AI technologies to work for society as a whole. Public trust is critical to the adoption of AI and consequently the growth of the AI sector, but that risks being undermined if individuals feel they are not adequately protected or treated fairly. As an example, The Perception of Fairness of Algorithms and Proxy Information in Financial Services report conducted an experiment showing people responded negatively (leaving a bank) when they realised the bank used algorithmic systems relying on proxies for gender or ethnicity.

104. This consultation considers whether there are shortcomings in the legislative framework and the tools available to help individuals meaningfully understand the inferences, often based on specific characteristics or attributes, made about them. Data protection is not the only relevant legislative framework in this fast-evolving landscape, and the government wants to consider its role in addressing the challenges and opportunities arising from algorithmic decision-making and profiling.

105. The UK GDPR contains definitions of 'personal data' and 'special category data'. These concepts arguably struggle to account for the fact that personal data takes on a life of its own, including through inferences, once it is captured in an AI system. The ICO, in its guidance on personal data, sets out that 'opinions and inferences are also personal data, maybe special category data, if they directly or indirectly relate to that individual' but that relation is not always straightforward. Organisations do not always understand the concepts of inferred and collective data, the privacy and other risks they can give rise to, and the practical steps they can take to identify, manage and process these data in a fair, lawful and transparent way.

106. Attempting to regulate 'inferred data' as a separate regulatory category would be counterproductive as the risk of harm to data subjects comes not from the data itself, but from the process and application in given use cases. For example, knowing an individual lives in a particular postcode (and may fit a certain income bracket) in and of itself is not particularly intrusive or harmful; it is only where that information is linked to a specific processing activity impacting the individual in a meaningful way that a risk of harm arises. There is therefore a spectrum of risk to navigate.

107. Article 13 of the UK GDPR describes in detail the transparency requirements for data controllers when they collect personal data directly from the data subject. At the time data is collected, the controller must provide the data subject with information about the purposes for which the data will be processed, and any potential third-party recipients. Given this sequence, it has been argued that Article 13 by definition covers only data provided by the data subject, including observed data, and that subsequently inferred or derived data cannot be included in the

[31] For instance, see Taylor, L., Floridi, L., & Van der Sloot, B. (Eds.). (2016). Group privacy: New challenges of data technologies (Vol. 126). Springer. and Mittelstadt, B. From Individual to Group Privacy in Big Data Analytics. Philos. Technol. 30, 475–494 (2017).

disclosure to the data subject as it has not yet been created.[32] There are also limits to the feasibility of providing real time notifications every time an inference is made, but there might be other ways to give individuals greater insight into high-risk inferences.

108. The Right of Access (Article 15) in the UK GDPR, which gives individuals the right to obtain a copy of their personal data, is enacted through individual 'subject access requests'. These requests are submitted to controllers by individuals, but do not have a standard format and are tasked only with revealing information relevant to an individual - they may not reveal inferences made, or potentially resulting patterns of discrimination. They also pertain only to access to information held about an individual and do not create a right to obligate the release of data about groups to which different groups may then have access.

109. Recital 71 to Article 22 UK GDPR states that data subjects should be able 'to obtain an explanation of the decision reached', and mentions statistical accuracy in the context of profiling and automated decision-making. The ICO stipulates that organisations making inferences must also provide meaningful information about the logic involved and what the likely consequences are for individuals.[33] The Recital states that organisations should put in place 'appropriate mathematical and statistical procedures' for the profiling of individuals as part of their technical measures. They should ensure any factors that may result in inaccuracies in personal data are corrected and the risk of errors is minimised. The recitals to the UK GDPR are not legally binding and there is no clear nor standardised explanation on what these procedures should include, despite the ICO's guidance.

110. Data Protection Impact Assessments can provide a structured approach for organisations to assess issues of fairness and human rights (including the rights and freedoms of data subjects) 'where the processing may give rise to discrimination', as outlined in ICO guidance. However, there may be limitations to the utility of Data Protection Impact Assessments as a safeguard against perpetuating bias, and there is a question as to whether impact assessments are the best place to address these questions. Data Protection Impact Assessments also fit into a wide array of impact assessments, such as Equality Impact Assessments and the emerging field of algorithmic impact assessments. These impact assessments all address related factors - but are not unified in one, standardised assessment for specific use cases.

111. The government recognises that there is ongoing activity in this area, and helpful initiatives to draw on, such as the ICO's AI Auditing framework, the Explaining Decisions Made with Artificial Intelligence guidance as developed in partnership with the Alan Turing Institute, and the Office for AI, Turing Institute and Government Digital Service's Understanding AI Ethics and Safety guidance.

112. There may be merit in enhancing the approach to explainability and accountability for fair processing as a lot of the concerns around inferred data arise from profiling generated by AI systems drawing inferences from an array of data points using complex algorithms. This should be considered as part of a holistic approach to govern AI which could enhance the many protections already offered in the UK GDPR. This will be considered further as part of the National AI Strategy, but, as part of this consultation, the government wants to establish the role of data protection legislation in increasing public trust in the use of AI systems.

[32] Sandra Wachter & Brent Mittelstadt, 'A Right to Reasonable Inferences: Rethinking Data Protection Law in the Age of Big Data and AI', p. 52, 2019

[33] ICO Guidance: What else do we need to consider if Article 22 applies?

The government welcomes views on the following issues:

Q1.5.18. Please share your views on the effectiveness and proportionality of data protection tools, provisions and definitions to address profiling issues and their impact on specific groups (as described in the section on public trust in the use of data-driven systems), including whether or not you think it is necessary for the government to address this in data protection legislation.

Q1.5.19. Please share your views on what, if any, further legislative changes the government can consider to enhance public scrutiny of automated decision-making and to encourage the types of transparency that demonstrate accountability (e.g. revealing the purposes and training data behind algorithms, as well as looking at their impacts).

Q1.5.20. Please share your views on whether data protection is the right legislative framework to evaluate collective data-driven harms for a specific AI use case, including detail on which tools and/or provisions could be bolstered in the data protection framework, or which other legislative frameworks are more appropriate.

113. Further work is underway, as part of the National AI Strategy and Centre for Data Ethics and Innovation's AI Assurance workstream, to assess the need for broader algorithmic impact assessments. The responses to the above questions will inform that work. This consultation document also covers algorithmic transparency in the public sector specifically, detailed in section 4.4.

1.6 Data Minimisation and Anonymisation

114. The UK's data protection legislation requires that personal data is adequate, relevant and limited to what is necessary, or not excessive, in relation to the purposes for which it is processed; this is commonly known as the data minimisation principle. This principle requires, for example, that organisations employ methods for processing that achieve their ends without making use of personal data unnecessarily.

115. Data minimisation techniques, such as pseudonymisation, can be applied to safeguard personal data, which in turn may allow for such data to be shared in safer ways. Sharing data openly but safely can be highly valuable - for example, in the research community it can allow for cross-validation of scientific results, significantly improving the reliability of findings.

116. Personal data is defined as any information relating to an identified or identifiable individual. There is a spectrum of identifiability: the process of safeguarding a dataset with data minimisation techniques should make it less easy to use on its own or in combination with other information to identify a person either directly or indirectly. For example, pseudonymised data is personal data which has been put through a process so that it cannot be used to identify an individual without additional information. Personal data may also undergo the process of anonymisation, so that an individual is not or no longer identifiable.

117. The distinction between anonymised and pseudonymised data is important because it delimits the scope of data protection legislation, including the UK GDPR. Pseudonymised data falls within the scope of data protection legislation, whereas anonymous data is not.

118. Determining whether personal data is anonymous may be complex; organisations must make a context-specific decision, taking into account various risks and external factors. The thresholds for determining anonymisation are arguably unclear, even for sectors where anonymisation is a fundamental part of data use and sharing, such as the research community. These thresholds are dynamic and change, for example, with the development of new techniques both to safeguard data and to re-identify it.

119. As a result, organisations may incorrectly classify data as anonymous and therefore fail to adequately protect personal data. Alternatively, organisations may apply anonymisation techniques to a greater extent than is necessary to mitigate risks to an individual's data protection rights, potentially compromising the value of the data set for re-use. Overuse of the anonymisation procedure may also be driven by the perceived risk of enforcement action in the event that a dataset is treated as anonymous but later used, possibly by a malevolent actor, to identify a person.

120. The government believes more could be done to help organisations understand what needs to be done to anonymise data. Organisations that have carried out appropriate due diligence to ensure that the data is reasonably unlikely to be re-identified should be able to realise its benefits. A proposed approach is set out in the following sections.

Clarifying the circumstances in which data will be regarded as anonymous

121. The UK's data protection legislation only regulates information relating to an identifiable living individual: it does not regulate anonymous information. At the moment, the legislation does not include a clear test for determining when data will be regarded as anonymous. There is, however, some guidance in the ICO's code of practice on anonymisation and in the recitals to the UK GDPR to help in determining whether data is anonymous. **In the interests of certainty, the government is proposing to place such a test onto the face of legislation, and is considering two options:**

    a. **Placing Recital 26 of the UK GDPR onto the face of legislation.** Recital 26 states that to determine whether a person is identifiable, account should be taken of 'all the means reasonably likely to be used' to (re-)identify the person, including all objective factors, such as costs and time required for identification, in light of available technology at the time of the processing and technological developments.

    b. **Creating a statutory test based on the wording of the Explanatory Report accompanying the Council of Europe's modernised Convention 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) (Convention 108+).** This explains that data will be regarded as anonymous when it is impossible to re-identify the data subject or if such re-identification would require unreasonable time, effort or resources, assessed on a case by case basis taking into consideration the purpose of the processing and objective criteria such as the cost, the

benefits of identification, the type of controller, the technology and so on, noting that this may change in light of technological and other developments.[34]

122. Either of these options would provide a clearer test for determining when data will be regarded as anonymous, and the government welcomes views on their benefits and risks.

Clarifying that the test for anonymisation is a relative one

123. **In addition to the proposals outlined above, the government is considering legislation to confirm that the question of whether data is anonymous is relative to the means available to the data controller to re-identify it.** The Court of Justice of the European Union (CJEU) favoured a relative approach when assessing whether dynamic IP addresses constitute personal data in the case of Breyer vs Germany. The Court noted it was relevant to ask what means of identification were available to the relevant controller processing the data, including where the relevant means of identification were in the hands of a third party from whom the controller could reasonably obtain them. If the data controller has no way of obtaining the means of identification, the data is not identifiable in the hands of the controller (and so is anonymous in that particular controller's hands even though it may be identifiable in another controller's hands).

124. The confirmation of a relative test for re-identification would not change the current position that the test may apply differently over time (owing to technological developments, for example), so organisations would continue to be expected to carry out appropriate due diligence to remain compliant. Furthermore, it would maintain the current position that the status of data - that is, whether it is anonymous or not - can be different depending on whose hands it is in. Organisations would therefore still have to consider whether data could be re-identified when shared with third parties. However, a relative test could give organisations more confidence to anonymise data and use it more innovatively within their own organisations, or when shared with organisations that adhere to similar standards on anonymisation and re-identification.

125. Greater use of effective anonymisation could help to better protect individuals' personal information, reduce risks for organisations and provide the opportunity for broader economic and societal benefits through an increase in the availability of data. Forthcoming guidance from the ICO on anonymisation, pseudonymisation and privacy-enhancing technologies (PETs) will also look to help organisations build confidence in the use of de-identification measures and any subsequent decisions to share data with third parties. The government is not currently planning any further legislative reform to better support use and standards of PETs beyond the proposals on anonymisation outlined above, but would welcome views on whether there are other areas it should explore.

The government welcomes views on the following questions:

Q1.6.1. To what extent do you agree with the proposal to clarify the test for when data is anonymous by giving effect to the test in legislation?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*

[34] Council of Europe Treaty Series - No. 223, 'Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', paras 17-20, 2018

- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q1.6.2. What should be the basis of formulating the text in legislation?

- *Recital 26 of the UK GDPR*
- *Explanatory Report to the Modernised Convention 108+*
- *N/A - legislation should not be amended*
- *Other*

Please explain your answer, and provide supporting evidence where possible.

Q1.6.3 To what extent do you agree with the proposal to confirm that the re-identification test under the general anonymisation test is a relative one (as described in the proposal)?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q1.6.4. Please share your views on whether the government should be promoting privacy-enhancing technology, and if so, whether there is more it could do to promote its responsible use.

1.7 Innovative Data Sharing Solutions

126. Alongside the legislative reforms already outlined in this chapter, the government wishes to encourage innovation in the way data can be shared. Increased use of data sharing solutions can help to drive growth and boost innovation by providing ways to manage and use data more efficiently. Such practices could see the benefits that, for example, better use of data in Open Banking unlocked for consumers replicated in other sectors. The government aims to encourage solutions that increase organisations' confidence and expertise in responsible data sharing practices.

Case Study: *Smart Data Open Banking scheme*

The UK's Open Banking scheme was the first of its kind globally and is the UK's most advanced Smart Data scheme set up to bring more competition and innovation to financial services. With customers' permission, Open Banking regulations mandate banks to allow the sharing of financial data with authorised providers such as budgeting apps and other banks. Over 3 million consumers and businesses use Open Banking to save time, money and effort.

Smart Data aims to build on an individual's right to data portability, enabling consumers (and businesses) to share their data easily and securely, when they choose, with authorised third-party providers. These providers then use this data to provide innovative services for the consumer or business user, such as automatic switching or better account management.

There is clear potential to broaden these benefits across further sectors and extend the UK's leading position. Greater personal data mobility could increase UK GDP by an estimated £27.8 billion in total, not including the wider contribution from any digital innovations enabled.[35]

The government has committed to extending its powers to mandate participation in Smart Data schemes, increasing the overall portability of data and the innovative use of the data which in turn improves both consumers' and business users' experience and provides them with financial savings.

127. This section invites views on the government's work to support innovative data sharing solutions, while maintaining protections for individuals.

Data intermediaries

128. The government aims to maximise the ease with which organisations can share and process data responsibly. The government recognises that these practices require a set of skills, knowledge and resources that not every organisation will have available in-house. Enabling more organisations to readily access these skills and resources could help to increase confidence in using data. A third party organisation may also act independently by ensuring that individual data subjects' rights are observed and protected whilst managing different parties' competing interests. Increasing the availability and use of specialist third-party data intermediaries would provide more widespread access to the right skills and resources, so more organisations can make better use of data. Data intermediaries can help with data stewardship - managing data collection, sharing, access and use in a responsible and efficient manner.

129. In certain cases, commissioning an independent data intermediary to perform data stewardship activities could enable responsible and lawful data sharing that would not be possible without the presence of a fully independent third party. A report by the Centre for Data Ethics and Innovation on what data intermediaries can offer, published in July 2021, provides several case studies and future opportunities.

Explanatory box: *What are data intermediaries?*

Each time data is shared, accessed, used or protected, a number of stewardship activities would typically take place at the intersection of the data sharing and access journeys. They can include, for example, finding data that is fit-for-purpose, managing transfers and usage rights, and ensuring that the right protections are in place.

Data intermediaries - operating in the public, private or third sectors - could help absorb

[35] DCMS, 'Data Mobility: The personal data portability growth opportunity for the UK economy', 2018

some of the costs and risks that would be normally associated with performing data processing activities in-house. There is already a vibrant ecosystem of innovative data intermediaries, which act between those sharing and accessing data. Many of these organisations are creating novel, technology-enabled solutions to allow safe and frictionless data sharing.

Data intermediaries can provide technical infrastructure and expertise to support interoperability between datasets, or act as a mediator negotiating sharing arrangements between parties looking to share, access or pool data. They can also provide rights-preserving services - for example, by acting as a data custodian allowing remote analysis through privacy-enhancing technologies, or providing independent analytical services in a siloed environment.

Data intermediaries could assume the roles and obligations of a data controller and / or processor, depending on the circumstances. Types of data intermediaries include:

- Data trusts, which can provide fiduciary data stewardship on behalf of data subjects (see also the joint Ada Lovelace/AI Council Legal Mechanisms for Data Stewardship report)
- Data exchanges, online data platforms where datasets can be advertised and accessed - commercially or on a not-for-profit basis
- Personal information management systems, which seek to give data subjects more control over their personal data
- Industrial data platforms, providing shared infrastructure to facilitate secure data sharing and analysis between companies
- Data custodians which enable privacy-protecting analysis or attribute checks of confidential data, for example via the application of privacy enhancing technologies
- Data cooperatives, which can enable shared data spaces controlled by data subjects
- Third parties trusted by those sharing and accessing data provide assurance to those looking to access confidential datasets that the data is fit-for-purpose - e.g. in terms of quality or ethical standards

130. Data intermediaries may also help support delivery and manage risk for some of the data protection proposals set out in this consultation. For example, they could help 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.

Case study: *OpenSAFELY*

OpenSAFELY is a highly secure, transparent, open-source software platform for analysis of electronic health records data. It can be deployed to create a Trusted Research Environment (TRE) alongside appropriate database, compute, governance, and administrative elements;

or it can be deployed as a privacy-enhancing layer on any existing secure database or TRE. OpenSAFELY software is currently deployed within the secure data centres of the two largest electronic health record providers in the NHS, to support urgent research into the Covid-19 emergency: thereby creating OpenSAFELY-TPP and OpenSAFELY-EMIS - covering the records of more than 95% of the UK population and enabling analysis that has been critical to the response to COVID-19.

OpenSAFELY enables secure analysis because it does not move patient data outside of the secure environments where it already resides and is managed on behalf of the NHS by electronic health record companies. Instead, trusted, named analysts with a credible track record can run large scale analysis across pseudonymised patient records in situ, and in near-real-time. In addition, all platform activity is publicly logged; all software for data management and analysis is shared, automatically and openly, for scientific review and efficient re-use. These combined features allow patients, professionals and the public to hold the entire system accountable.

131. Despite their clear potential, and established benefit in some sectors, the development of many types of data intermediaries - such as those providing confidential data sharing solutions - remains nascent. There is a risk that this is leading to missed opportunities to share, access and use data where there is a public interest or economic value in doing so. Data intermediaries face a number of challenges because there is not yet an established market framework for their operation, which could help to create confidence in the rules of engagement and provide mechanisms for managing risk.

132. Data intermediaries may be experiencing uncertain demand for their services, stemming from lack of awareness of the opportunity and services they provide, and lack of confidence in how data intermediaries might use their privileged access to data. There may also be uncertainty about what data intermediaries can do on behalf of data controllers and how data controllers can have confidence in data intermediaries' services.

133. Data intermediaries themselves are governed by the data protection legislative framework, which all organisations are required to comply with and, as such, are exposed to legal compliance risk, which may also have implications for the original data controller. And just like others in the data economy, data intermediaries and users of their services have to contend with the costs associated with foundational data management challenges (identified in the National Data Strategy - affecting how findable, accessible, interoperable and reusable data is), including lack of coordination on standards and infrastructure.

134. There is some uncertainty about the architecture of any data flow ecosystem that will ultimately emerge - particularly the path that data follows when flowing from data subjects or those collecting data to users, and how data intermediaries and technologies could mediate this process. This will have implications for risk, user experience and the public benefit of data use.

135. The government is considering how it might support the activities of data intermediaries in order to deliver more innovative data sharing solutions and enable more responsible and legally compliant data sharing. Different measures may be needed to support the development of different data intermediaries in different sectors or taking on different roles in the data sharing ecosystem, such as: stewarding confidential data; stewarding data that will be used to inform

important decisions affecting commercial, public or personal outcomes; stewarding data between different data ecosystems; providing novel data sharing and governance solutions; or operating in markets with an incumbent. Intermediaries, like any organisation processing confidential data, would still need to manage risks appropriately and act lawfully.

136. There are a number of ways the government could intervene to support data intermediaries, as set out in Policy Lab's Styles of Government Action – including as a collaborator, steward, customer, provider, funder, regulator and legislator. Government intervention - such as voluntary or compulsory accreditation evidenced by audits; an enforceable code of practice; activity reporting requirements; or data intermediary uptake incentives - could help data intermediaries signal the quality, lawfulness and responsibleness of the services that they provide, ensure responsible and trusted data use, empower data originators, enable low-friction data flows, and support the development of healthy markets.

137. The government seeks to support and engender confidence in the uptake of data intermediaries in high public-interest applications, and support data collection, sharing, pooling and access where the same privacy standards would not have been achieved without an independent third party creating a barrier between the data and other activities. We would like to better understand the lawful grounds that might be used for the stewardship activities performed by data intermediaries, as well as the conferring of data processing rights and responsibilities to those data intermediaries. We are exploring under what circumstances consent might be the only appropriate lawful ground, and what predefined criteria would have to be met to remove the need for recourse to consent. Lastly, there is merit in considering how a code of conduct and/or accreditation might be leveraged to place specific conditions on data intermediaries, and whether/how it could allow them to provide confidence that they are conducting those activities in a responsible manner.

The government welcomes views on the following questions:

Q1.7.1. Do you think the government should have a role enabling the activity of responsible data intermediaries?

- *Yes*
- *No*
- *Don't know*

Please explain your answer, with reference to the barriers and risks associated with the activities of different types of data intermediaries, and where there might be a case to provide cross-cutting support). Consider referring to the styles of government intervention identified by Policy Lab - e.g. the government's role as collaborator, steward, customer, provider, funder, regulator and legislator *- to frame your answer.*

Q.1.7.2. What lawful grounds other than consent might be applicable to data intermediary activities, as well as the conferring of data processing rights and responsibilities to those data intermediaries, whereby organisations share personal data without it being requested by the data subject?

Please explain your answer, and provide supporting evidence where possible, including on:

- *If Article 6(1)(f) is relevant, i) what types of data intermediary activities might constitute a legitimate interest and how is the balancing test met and ii) what types of intermediary activity would not constitute a legitimate interest*
- *What role the government should take in codifying this activity, including any additional conditions that might be placed on certain kinds of data intermediaries to bring them within scope of legitimate interest*
- *Whether you consider a government approved accreditation scheme for intermediaries would be useful*

1.8 Further Questions

Q1.8.1. In your view, which, if any, of the proposals in 'Reducing barriers to responsible innovation' would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

Q1.8.2. In addition to any of the reforms already proposed in 'Reducing barriers to responsible innovation' (or elsewhere in the consultation), what reforms do you think would be helpful to reduce barriers to responsible innovation?

Chapter 2 - Reducing burdens on businesses and delivering better outcomes for people

2.1 Introduction

138. The government's plan for growth, Build Back Better, makes a commitment to develop an agile regulatory approach that supports innovation, and protects citizens and the environment. Our principles for regulation in the Plan for Digital Regulation include actively promoting innovation, achieving forward-looking and coherent outcomes, and addressing international opportunities and challenges. This is particularly critical in the area of data where technological change is so rapid.

139. The government remains committed to high standards of data protection and wants a regulatory regime that delivers effectively without unnecessary burdens. The current legislation is based on a model that prescribes a series of activities and controls that organisations must adopt in order to be considered compliant. Although a key goal of the EU's GDPR was to create a regime that focussed on the accountability of organisations, the current model, in practice, tends towards a 'box-ticking' compliance regime, rather than one which encourages a proactive and systemic approach, and risks undermining the intentions of the principle of accountability. A largely one-size-fits-all approach from organisations, regardless of the relative risk of their data processing activities, can potentially discourage innovation in how to achieve the actual goals of using data responsibly and protecting individuals' rights.[36] Overall this approach might deliver worse outcomes for individuals while imposing unnecessarily high costs on organisations, as well as disincentivising the development of better practices.

140. The UK's future data protection regime will incentivise organisations to invest more effectively in the governance, policies, tools, people and skills that protect personal data, so individuals can have even greater confidence that their personal data is being used responsibly. The government wants organisations to focus on the right outcomes, freeing them up to implement effective data protection policies and processes. Our proposals will reduce burdens on organisations by, for example, equipping them with tools to more effectively respond to subject access requests and providing greater flexibility on compliance within the accountability framework. Proportionate and flexible compliance activities will help organisations unlock the value of their data assets rather than being seen as a regulatory burden.

141. Furthermore, the UK's future data protection regime will not require organisations to change many of their current processes if they already operate effectively, but it will provide the flexibility to do so if other processes can deliver the same or better outcomes in more innovative and efficient ways.

2.2 Reform of the Accountability Framework

142. A key driver of unnecessary burdens on organisations is the accountability framework set out in the UK GDPR. This framework is made up of the accountability principle (Article 5), as well as a number of specific requirements designed to help organisations demonstrate compliance with the other principles in the UK GDPR.

143. The accountability principle is recognised as a key building block of effective data protection regulation and implementation, featuring in the OECD Guidelines on the Protection of Privacy

[36] Martin et al: How Data Protection Regulation Affects Startup Innovation (2019)

and Transborder Flows of Personal Data, adopted in 1980. It is intended to support a number of outcomes, including: the protection of personal data; transparency; embedding data protection into organisational practices; enabling public trust; regulatory clarity and confidence in compliance; and facilitating enforcement activity.

144. While the principle of accountability is fundamental, the current legislative framework sets out a number of specific requirements that organisations must satisfy in order to demonstrate compliance. These rules may be generating a significant and disproportionate administrative burden, and leading organisations to misdirect time and energy away from the activities that ensure the responsible use of personal data in a specific context. This approach to compliance may also be putting a particularly disproportionate burden on SMEs and organisations that undertake low risk processing, despite some current requirements being risk-based and limited exemptions applying.

145. **To address this, the government is proposing to implement a more flexible and risk-based accountability framework which is based on privacy management programmes.** Under this framework, organisations would be required to implement a privacy management programme tailored to their processing activities and ensure data privacy management is embraced holistically rather than just as a 'box-ticking' exercise. Further details are set out in paragraph 156 below.

146. The UK's data protection regime will retain the principle of accountability at its heart, while enabling organisations to meet its high standards in ways that reflect how they operate and that satisfy their users' expectations.

147. **To support the implementation of privacy management programmes, the government proposes to amend or remove specific compliance requirements in the UK GDPR, which are disproportionately burdensome for many organisations.** Further details are set out in paragraph 159 below.

148. The government knows that many organisations have invested time and resources to establish policies and processes in order to comply with the UK GDPR. While many of the compliance activities currently undertaken by organisations would likely help to demonstrate compliance with any future accountability framework, the government believes there is an opportunity to create space for more innovative approaches. There is a balance to strike so that the accountability framework in legislation becomes more flexible and risk-based but does not inadvertently create uncertainty and compliance risks that organisations may find difficult to manage.

149. **To further support organisations that can demonstrate a proactive commitment to accountability under the proposed framework, the government is considering whether to introduce a new voluntary undertakings process** similar to Singapore's Active Enforcement regime. Further details are set out in paragraph 181 below.

150. The government recognises that some organisations may be better equipped than others to take advantage of greater flexibility to demonstrate compliance with the UK GDPR. A future approach will ensure that clear guidance from the ICO is available to organisations lacking the capacity or expertise to design their own accountability practices without support. Detailed guidance for organisations would not be written into legislation as it is relatively difficult to update in order to keep pace with best practice.

<u>Accountability based on privacy management programmes</u>

151. This proposal would require an organisation to develop and implement a risk-based privacy management programme that reflects the volume and sensitivity of the personal information it handles, and the type(s) of data processing it carries out. A privacy management programme would include the appropriate personal information policies and processes for the protection of personal information.

152. A privacy management programme is a framework intended to help an organisation establish a robust and risk-based approach to data protection management, which is embraced and embedded throughout its activities. Privacy management programmes are based on a number of elements at the core of accountability, such as: leadership and oversight, risk assessment, policies and processes, transparency, training and awareness of staff, and monitoring, evaluation and improvement.[37]

153. A privacy management programme is valuable in many ways. In designing and implementing a privacy management programme, organisations would need to consider their compliance policies and processes holistically and proportionally, and this should result in a more coherent, comprehensive and systemic approach to accountability. Organisations that have demonstrated this approach to accountability have seen competitive benefits and reputational advantages.[38] A privacy management programme should also provide assurance to the regulator and data subjects that the policies and processes in place are effective and demonstrate compliance.

154. This model is not a novel approach but has developed from core principles of effective accountability practices and best practice in industry. Other jurisdictions, such as Singapore, Australia and Canada, have accountability frameworks that are more flexible and risk-based than the UK GDPR, and include the operation of privacy management programmes. This proposal has drawn on these regimes.

155. There is currently no explicit requirement for organisations to implement a privacy management programme but Article 24 of the UK GDPR requires organisations that handle personal data to 'implement appropriate technical and organisational measures to ensure, and be able to demonstrate, that processing is performed in accordance with the legislation'. This must include the implementation of appropriate data protection policies, where proportionate, in relation to the organisation's processing activities. This proposal seeks to reinforce and expand on Article 24.

Case study: *Canada's approach to privacy management programmes, 'Getting Accountability Right with a Privacy Management Programme'*

The Office of the Privacy Commissioner of Canada (OPC), and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia have jointly developed a document with the goal of providing consistent guidance on what it means to be an accountable organisation. Their Getting Accountability Right with a Privacy Management Programme guidance sets out the development of a privacy management programme into two parts.

[37] An accountability mapping report by the Centre for Information Policy Leadership (CIPL), '*What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework'* (September 2019) outlined how a sample of organisations of different sectors, geographies and sizes implement effective data privacy management programmes that reflect the 'CIPL Accountability Framework' which is based on these seven core elements.

[38] CISCO: 'From Privacy to Profit: Achieving Positive Returns on Privacy Investments', Data Privacy Benchmark Study, 2020

- The accountability fundamentals: Organisational commitment and programme controls

- Ongoing assessment and revision: Developing an oversight and review plan and assessing and revising the programme controls

The guidance outlines what is considered by regulators as best practice guidelines for an effective privacy management programme for organisations of all sizes. The guidance makes clear, however, that this is not a 'one-size-fits-all' solution but can be used by organisations in all industries and of all different sizes.

156. The new, proposed accountability framework would require that organisations be accountable for personal information under their control and must:

    a. Develop and implement a privacy management programme which includes the appropriate policies and processes for the protection of personal information and, specifically, cover:

        I. The roles and responsibilities within the organisation in relation to personal data protection, including who is designated as the responsible individual(s) for the privacy management programme and overseeing the organisation's data protection compliance. The designated individual(s) will also be responsible for representing the organisation to the ICO and data subjects where necessary. The legislation would not prescribe the specific requirements needed for the role(s) and an organisation would have discretion over appointments, including by being able to determine the appropriate skills, qualifications and position needed for the role(s), taking account of the volume and sensitivity of the personal information under its control, and the type(s) of data processing it carries out.

        II. Evidence that oversight and support from senior management, and appropriate reporting mechanisms to senior management, are in place, and how the organisation ensures its staff understand key data protection obligations, policies and processes.

        III. Measures which assist the designated responsible individual(s) for structuring an appropriate privacy management programme and demonstrate the organisation is compliant with data protection legislation. These include:

            i. Personal data inventories which describe and explain what data is held, where it is held, why it has been collected and how sensitive it is

            ii. Internal policies that address the organisation's obligations under the data protection legislation

            iii. Risk assessment tools for the identification, assessment and mitigation of privacy risks across the organisation

            iv. Procedures for communicating with data subjects about their data protection rights and the organisation's policies and processes under a privacy management programme

v. How requests for information and complaints are received and dealt with

vi. Procedures for handling breaches

b. Operate plans and processes to monitor, assess, review and revise the privacy management programme periodically, as necessary.

c. In designing and implementing the privacy management programme, ensure that the volume and sensitivity of the personal information under its control, and the type(s) of data processing it carries out, have been taken into account.

d. Regularly examine the effectiveness and appropriateness of policies, processes and procedures to ensure they remain effective and appropriate, and update and amend them accordingly. To remain practical and effective, privacy management programmes need to adapt in order to keep current with changes in, for example, an organisation's data processing activities, administrative structures and the relevant legislation.

e. Make available, on request, their privacy management programme and accompanying documentation in order to enable the ICO to continue to enforce the legislation effectively.

f. Take all practical steps to ensure clear and easily understandable transparency of its policies and processes under a privacy management programme, including who should be contacted for any questions or concerns.

157. The ICO's Regulatory Action Policy sets out its approach to enforcement action, including any mitigating or aggravating factors it takes into account during investigations.[39] We would expect the Regulatory Action Policy to reflect the importance of accountability within the UK GDPR and treat failures to comply appropriately seriously. When taking enforcement action against any infringement of an organisation's data protection obligations, the ICO would be required to take into account the quality and effectiveness of a privacy management programme in determining any penalties or other action. Any organisation whose privacy management programme does not meet the required standards might be asked by the ICO, in the first instance, to make improvements to its privacy management programme.

158. The government believes that placing privacy management programmes at the heart of accountability also creates an opportunity to remove some unnecessarily prescriptive or burdensome requirements from legislation, as set out below. Nonetheless a strong privacy management programme is likely, in practice, to exhibit many of the same features as the current legislation. Organisations may wish to use many of their existing UK GDPR compliance practices to meet the requirements of a privacy management programme, preventing the need for significant additional investment in compliance activity.

159. **To support the implementation of the new accountability framework, the government proposes to remove and amend various requirements in the current legislation, as set out below.** Requirements of the current accountability regime that are not covered below would remain the same.

<u>Data protection officers</u>

160. Articles 37 to 39 of the UK GDPR set out the requirements on organisations to appoint a data protection officer, as well as the position and tasks of a data protection officer. Failing to appoint

[39] See reference: Data Protection Act 2018. Guidance about Regulatory Action. c. 12, PART 6, 160

a data protection officer can result in enforcement action, including a fine of up to the greater of £8.7 million or 2% of annual global turnover.

161. Organisations are required to appoint a data protection officer if they are a public authority (except for courts acting in their judicial capacity), or if certain types of processing activities are carried out. The data protection officer's tasks are to: inform and advise the organisation of their obligations under, and monitor compliance with, the UK GDPR and other data protection legislation; provide advice regarding data protection impact assessments, and; act as a point of contact with the ICO. The data protection officer must be independent: they may have other duties within the organisation but these must not result in a conflict of interests with their role as data protection officer. Therefore, data protection officers have a quasi-regulatory function within an organisation.

162. The current requirements do not necessarily drive the intended outcomes of the legislation. Some organisations may struggle to appoint an individual with the requisite skills and who is sufficiently independent from other duties, especially in the case of smaller organisations.

163. **The government therefore proposes to remove the existing requirements to designate a data protection officer.** The new proposed requirement to designate a suitable individual, or individuals, to be responsible for the privacy management programme and for overseeing the organisation's data protection compliance (see paragraph 156a(I)) would place different obligations on organisations, potentially driving more effective data protection outcomes.

164. There may be risks to removing the data protection officer role, if this were to significantly weaken internal scrutiny. However, organisations still need to be compliant with the data protection legislation and accountable for compliance. Indeed, some organisations - for example, those that undertake high-risk processing - may opt to designate an individual to perform a role similar to that of a data protection officer in order to independently monitor and assess the organisation's data protection compliance, particularly if an organisation believes this internal scrutiny would help demonstrate its commitment to the accountability principle. However, this would need to be in addition to the 'responsible individual(s)' that must be appointed as part of a privacy management programme (see paragraph 156a(I)).

<u>Data protection impact assessment</u>

165. Article 35 of the UK GDPR requires organisations to undertake a data protection impact assessment for processing likely to result in a high risk to individuals and sets out what the assessment must include. Failing to comply with this obligation where it arises can result in enforcement action, including a fine of up to the greater of £8.7 million or 2% of annual global turnover.

166. While data protection impact assessments are one of the ways in which an organisation can effectively identify, assess and minimise the data protection risks, organisations may identify other risk management practices which achieve the intended outcomes.

167. **The government therefore proposes to remove the requirement for organisations to undertake a data protection impact assessment, so that organisations may adopt different approaches to identify and minimise data protection risks that better reflect their specific circumstances.**

168. Removing this requirement may increase the risk that organisations will undertake processing that is high risk without an adequate prior assessment of the impact of the processing on the

protection of personal data and, as a result, may not identify and put in place appropriate safeguards. This would be mitigated by the requirements of the privacy management programme, whereby an organisation would be required to have in place risk management processes, including the processes which allow for the identification, assessment and mitigation of data protection risks across the organisation. The government anticipates that regulatory guidance would offer strategies that organisations should consider adopting to protect personal data, including when and how they may want to undertake a data protection impact assessment.

169. Existing data protection impact assessments would remain valid and the processing for which they were prepared would not need to be reassessed via new means.

Prior consultation with the Information Commissioner's Office

170. The government wants to encourage a more proactive, open and collaborative dialogue between organisations and the ICO on how to identify and mitigate risks, especially for high risk processing activities. The current legal provisions that seek to achieve this may not be resulting in the intended outcomes.

171. Article 36 (1)-(3) of the UK GDPR requires that, where an organisation has identified a high risk that cannot be mitigated, it must consult the ICO before starting the processing and may face enforcement action if it fails to do so, including penalties of up to the greater of £8.7 million or 2% of annual global turnover. Where the ICO is of the opinion that the intended processing would infringe the legislation, in particular where the organisation has insufficiently identified or mitigated the risk, the ICO can, within a period of up to eight weeks of receipt of the request for consultation, provide written advice to the organisation and may use its enforcement powers against the organisation. The government is aware, however, that prior consultation under Article 36 is infrequently used,[40] and that this could result from concern that Article 36 would lead to immediate enforcement action.

172. **The government therefore proposes to remove the requirement for prior consultation with the ICO so it is no longer mandatory and organisations would not face any direct penalties for failing to consult the ICO in advance of carrying out the processing.**

173. Removing this requirement may decrease the frequency of prior consultation with the ICO, however, given this is already infrequently used, the government considers the benefits may outweigh the risks by encouraging more proactive, open and collaborative dialogue between organisations and the ICO. Organisations should continue to seek advice and guidance from the ICO where they have identified a high risk and, to support organisations, the ICO will be required to set out a list of processing activities that it considers to be high risk to ensure clarity. To encourage and incentivise organisations to engage with the ICO for guidance on high risk processing, in the event of a future investigation, the ICO would take account of whether an organisation had approached it for advice as mitigating evidence that the organisation has demonstrated a proactive approach to accountability.

[40] Information about the frequency of the use of prior consultation with the ICO, under Article 36, provided by the ICO.

Record keeping

174. The current accountability framework sets out a requirement for organisations to maintain at all times a record of processing activities, which must include all of the information set out in Article 30 of the UK GDPR. This includes information on the purposes of the processing; the categories of data and categories of data subjects to which the processing relates; the organisations with whom the data might be shared, including in any third countries; and (where possible) how long the data will be kept for and what security measures are in place to protect it.

175. While there is an exemption in Article 30(5) for some organisations from these record-keeping requirements, it only applies to organisations with fewer than 250 employees, so long as their processing of personal data is 'not occasional'. Since most organisations will process some personal data routinely, even if this is just personal data relating to their employees or suppliers and customers, this means that most businesses will have to maintain Article 30 records.

176. This requirement can involve the creation of large amounts of paperwork, which largely duplicates information required by other provisions in the legislation, particularly the requirement to provide information to data subjects in Articles 13 and 14 of the UK GDPR. In addition, as part of a privacy management programme, an organisation would be required to have in place measures which assist the designated responsible individual for structuring an appropriate privacy management programme and demonstrate the organisation is compliant with data protection legislation. This includes having personal data inventories which explain what personal data is held, where it is held, why it has been collected and how sensitive it is (see paragraph 156a(III)).

177. **The government therefore proposes to remove record keeping requirements under Article 30.** The record keeping requirement under Article 30 may help organisations to improve their data governance, comply with other aspects of the UK GDPR and assist with regulatory enforcement. There are risks that removing the requirements under Article 30 could hinder effective enforcement and offer less regulatory protection to data subjects. However the government considers the risks to be minimal. The new requirements under a privacy management programme would still require certain records be kept but organisations will have more flexibility about how to do this in a way that reflects the volume and sensitivity of the personal information they handle, and the type(s) of data processing they carry out. In addition, Articles 13 and 14 of the UK GDPR will still require much of the same information to be recorded in privacy notices.

Breach reporting

178. Breach reporting requirements are set out under Article 33 of the UK GDPR. Currently, under Article 33 (1), an organisation must inform the ICO of a data breach 'unless the personal data breach is unlikely to result in *a risk* to the rights and freedoms of natural persons' (emphasis added). This exemption can only be relied upon where there is likely to be no risk to an individual's rights and freedoms, so even breaches which present a low risk would be notifiable.

179. A low legal threshold for reporting and incentives for organisations to over-report (likely to be due to the possibility of regulatory action by the ICO and reputational damage for failing to comply with the obligation to report) mean that organisations report breaches to the ICO which are not likely to result in a risk to individuals' rights and freedoms. This over-reporting is costly in terms of time, effort and money for organisations as well as causing a significant workload for the ICO.

180. **To address the problems outlined above, the government is considering whether to change the threshold for reporting a data breach to the ICO so that organisations must report a breach unless the risk to individuals is not material**. The government would encourage the ICO to produce guidance and examples of what constitutes a 'non material' risk, as well as to produce examples of what is and what is not reportable, in order to assist organisations. Breaches of the new reporting threshold would result in the same sanctions as under the current regime, carrying maximum fines of the greater of £8.7m or 2% of annual worldwide turnover. Adjusting the threshold for breach reporting may increase the risk that organisations report fewer breaches, including those that are likely to result in a risk to an individual's rights and freedoms. However, given the current tendency for over-reporting and the unnecessary burdens this places on organisations and the ICO, the government considers the benefits may outweigh the risks.

181. **In order to further support organisations who can demonstrate a proactive commitment to accountability, the government is considering whether to introduce a new voluntary undertakings process, similar to Singapore's** Active Enforcement regime**.** Only organisations that are able to demonstrate they have embraced a proactive approach to accountability (for example, an organisation has evidence of engagement or prior consultation with the ICO ahead of high risk processing) would be able to provide the ICO with a remedial action plan, upon discovering an infringement, which could be accepted as part of the voluntary undertakings process. Provided that the plan then meets certain criteria - for example, it identifies the likely cause(s) of the incident, and proposes effective and timely steps to address the cause(s) - the ICO may authorise the plan without taking any further action.

182. The government is aware that the introduction of privacy management programmes may create additional burdens for organisations arising from increased discretion as to how to deliver compliance within the new accountability framework. However, the government expects regulatory guidance on the implementation of privacy management programmes will set out regulatory expectations and dispel uncertainty about the operation of the new system. Guidance could also address any possible risks, and accompanying safeguards that should be put in place, to ensure a high level of protection of individual's personal data under the new approach, on which the government welcomes views.

183. The ICO's Accountability Framework guidance lays the foundations of a privacy management programme, therefore some organisations may already have implemented a privacy management programme, or similar. However, making a new requirement for all organisations to implement privacy management programmes will encourage consistency and ensure that all organisations have approached privacy and data protection management in a systemic, proportionate and risk-based way.

The government welcomes views on the following questions:

Privacy management programmes

Q2.2.1. To what extent do you agree with the following statement: 'The accountability framework as set out in current legislation should i) feature fewer prescriptive requirements, ii) be more flexible, and iii) be more risk-based'?

- *Strongly agree*

- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q2.2.2. To what extent do you agree with the following statement: 'Organisations will benefit from being required to develop and implement a risk-based privacy management programme'?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible and in particular:

- *Please share your views on whether a privacy management programme would help organisations to implement better, and more effective, privacy management processes.*
- *Please share your views on whether the privacy management programme requirement would risk creating additional burdens on organisations and, if so, how.*

Q2.2.3. To what extent do you agree with the following statement: 'Individuals (i.e. data subjects) will benefit from organisations being required to implement a risk-based privacy management programme'?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your choice, and provide supporting evidence where possible.

- *Please share your views on which, if any, elements of a privacy management programme should be published in order to aid transparency.*
- *What incentives or sanctions, if any, you consider would be necessary to ensure that privacy management programmes work effectively in practice.*

Data protection officer requirements

Q2.2.4. To what extent do you agree with the following statement: 'Under the current legislation, organisations are able to appoint a suitably independent data protection officer'?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your choice, and provide supporting evidence where possible.

Q2.2.5. To what extent do you agree with the proposal to remove the existing requirement to designate a data protection officer?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q.2.2.6. Please share your views on whether organisations are likely to maintain a similar data protection officer role, if not mandated.

Data protection impact assessments

Q2.2.7. To what extent do you agree with the following statement: 'Under the current legislation, data protection impact assessment requirements are helpful in the identification and minimisation of data protection risks to a project'?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q.2.2.8. To what extent do you agree with the proposal to remove the requirement for organisations to undertake data protection impact assessments?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible, and in particular describe what alternative risk assessment tools would achieve the intended outcome of minimising data protection risks.

Prior consultation requirements

Q. 2.2.9 Please share your views on why few organisations approach the ICO for 'prior consultation' under Article 36 (1)-(3). As a reminder Article 36 (1)-(3) requires that, where an organisation has identified a high risk that cannot be mitigated, it must consult the ICO before starting the processing.

Please explain your answer, and provide supporting evidence where possible.

Q.2.2.10. To what extent do you agree with the following statement: 'Organisations are likely to approach the ICO before commencing high risk processing activities on a voluntary basis if this is taken into account as a mitigating factor during any future investigation or enforcement action'?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible, and in particular: what else could incentivise organisations to approach the ICO for advice regarding high risk processing?

Record keeping

Q.2.2.11. To what extent do you agree with the proposal to reduce the burden on organisations by removing the record keeping requirements under Article 30?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Breach reporting requirements

Q.2.2.12. To what extent do you agree with the proposal to reduce burdens on organisations by adjusting the threshold for notifying personal data breaches to the ICO under Article 33?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible and in particular:

- *Would the adjustment provide a clear structure on when to report a breach?*
- *Would the adjustment reduce burdens on organisations?*
- *What impact would adjusting the threshold for breach reporting under Article 33 have on the rights and freedoms of data subjects?*

Voluntary undertakings process

Q.2.2.13. To what extent do you agree with the proposal to introduce a voluntary undertakings process? As a reminder, in the event of an infringement, the proposed voluntary undertakings process would allow accountable organisations to provide the ICO with a remedial action plan and, provided that the plan meets certain criteria, the ICO could authorise the plan without taking any further action.

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Further questions

Q.2.2.14. Please share your views on whether any other areas of the existing regime should be amended or repealed in order to support organisations implementing privacy management requirements.

Q.2.2.15. What, if any, safeguards should be put in place to mitigate any possible risks to data protection standards as a result of implementing a more flexible and risk-based approach to accountability through a privacy management programme?

184. **If the government chooses not to pursue the implementation of privacy management programmes, certain elements of this proposal could be implemented as stand-alone reforms:**

a. The proposals on data protection impact assessments (paragraph 167), prior consultation with the ICO (paragraph 172) and voluntary undertakings process (paragraph 181), would only be implemented alongside the introduction of privacy management programmes

b. The proposal to amend breach reporting requirements (paragraph 180) could be taken forward regardless of whether privacy management programmes are implemented

c. The proposal to repeal record keeping requirements (paragraph 177) would not be implemented in full, but certain elements of the current record keeping requirements under Article 30 could be amended in order to reduce burdens on organisations, for example where the record keeping requirement duplicates requirements in other provisions in the legislation, such as the requirements to provide information to data subjects in Articles 13 and 14 of the UK GDPR.

d. The proposal to repeal the data protection officer requirement (paragraph 163) would not be implemented in full. An alternative is to remove **the requirement for all public authorities to appoint a data protection officer.**

    I. As set out in paragraph 160, public authorities (excluding courts) are required by the UK GDPR to appoint a data protection officer. This is a 'one-size-fits-all' model that applies to all public authorities, regardless of how much personal data is processed and the specific risks to individuals' rights and freedoms**.**

    II. A more risk-based approach is already applied to private companies. Broadly speaking, other bodies need only appoint a data protection officer if their core activities consist of large-scale monitoring of data subjects, or large-scale use of sensitive data or data involving criminal convictions. This approach is of particular benefit to small and micro businesses which can save on the costs of appointing a data protection officer if their core activities do not involve those elements. In contrast, public authorities whose core activities also do not involve those elements are unable to make the same savings.

    III. Employing a data protection officer can be particularly expensive for small public authorities. If small public authorities are engaging in processing that presents low risks to individuals' rights and freedoms, employing a data protection officer may be disproportionate, especially if they are processing low volumes of personal data.

    IV. The government assesses that it might be proportionate to remove the one-size fits-all requirement and instead take greater account of the individual risks posed by each public authority's processing. This approach presents various challenges to consider, such as how 'low volume' or 'low risk' should be determined. Low volume may not always mean low risk: processing by public authorities may still present risks that are often inherently different to those associated with private bodies' processing. There may also be a general advantage to maintaining the requirement for all public authorities to appoint a data protection officer in terms of improved compliance and public confidence, even if they are only processing mostly non-sensitive personal data on a small scale.

V. If the government did not pursue the implementation of privacy management programmes, there are two options to reform the current data protection officer requirements for public authorities:

i. **Allow public authorities to follow the same approach as other organisations for determining whether it is necessary to appoint a data protection officer.** This would mean removing 'being a public authority' from the list of automatic triggers for appointing a data protection officer. Rather than a one-size-fits-all approach, public authorities would only be required to make such an appointment if their core activities consist of large-scale monitoring of data subjects or large-scale use of sensitive data or data involving criminal convictions. The government would encourage the ICO to update its guidance on data protection officers to help public authorities determine their risk thresholds. However, there is a possibility that large public authorities' future processing may intrinsically present certain risks to individuals yet fall short of the specific criteria for requiring a data protection officer.

ii. **Retain a requirement for public authorities to appoint a data protection officer but limit its scope to authorities meeting certain criteria.** This could alleviate the burden on small public authorities where it is at its most disproportionate, while retaining the requirement for public authorities where it may be still beneficial even when their core activities are not large-scale monitoring or large-scale use of sensitive data. The challenge would be how the criteria are selected. Possible criteria could include the volume of the data, the size of the body, and aspects of the processing such as whether it is for the purpose of making decisions affecting the data subjects.

The government welcomes views on the following questions, relating to alternative reform proposals should privacy management programmes not be introduced:

Record-keeping

Q2.2.16. To what extent do you agree that some elements of Article 30 are duplicative (for example, with Articles 13 and 14) or are disproportionately burdensome for organisations without clear benefits?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible, and in particular address which elements of Article 30 could be amended or repealed because they are duplicative and/or disproportionately burdensome for organisations without clear benefits.

Breach reporting requirements

Q.2.2.17. To what extent do you agree that the proposal to amend the breach reporting requirement could be implemented without the implementation of the privacy management programme?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Data protection officers

Q.2.2.18. To what extent do you agree with the proposal to remove the requirement for all public authorities to appoint a data protection officer?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q.2.2.19. If you agree, please provide your view which of the two options presented at paragraph 184d(V) would best tackle the problem.

Please provide supporting evidence where possible, and in particular:

- *What risks and benefits you envisage*
- *What should be the criteria for determining which authorities should be required to appoint a data protection officer*

Further questions

Q2.2.20 If the privacy management programme requirement is not introduced, what other aspects of the current legislation would benefit from amendments, alongside

the proposed reforms to record keeping, breach reporting requirements and data protection officers?

2.3 Subject Access Requests

185. The right of access is one of the fundamental rights in data protection legislation and the government will protect it. Subject access requests are a critical transparency mechanism under this right, allowing individuals to check the accuracy of their personal data, learn more about how their data is being used and with whom their data is being shared, and obtain a copy of the data held about them.[41] Individuals have a right to appoint a third party to act on their behalf, if they wish.

186. The government and the ICO are aware that some organisations have experienced a number of issues with the ways that subject access requests are submitted and handled. These issues fall into two broad categories:

    a. Organisations' capacity to process requests: processing subject access requests can be time-consuming for organisations, taking up significant levels of resource. This is exacerbated in circumstances where the volume of requests is high ('bulk requests'). Smaller organisations might have fewer resources available to respond to these requests.

    b. Threshold for responding to a request: Recital 63 to the UK GDPR states that the purpose of a subject access request is to allow a data subject to 'be aware of, and verify, the lawfulness of the processing' of personal data. In some cases, subject access requests may be used in ways whereby the processing of personal data does not appear to be the sole or primary reason for exercising the right of access. For example, there is a risk that subject access requests may be used as a means of circumventing strict disclosure (of information and inspection of documents) protocols that would otherwise need to be followed under the Civil Procedural Rules in the context of actual or prospective litigation.[42] As set out in guidance by the ICO, the general position under current law is that a controller cannot consider the purpose of a subject access request unless it seems apparent that the request is 'manifestly unfounded', whereby the data subject has no intention of exercising their right of access, or where the subject access request is 'malicious in intent' and is 'being used to harass an organisation with no real purpose other than to cause disruption'.[43] The government is aware that some organisations believe that the threshold of 'manifestly unfounded' makes it difficult for data controllers either to navigate instances in which it would be appropriate to enquire about the purpose of the request, or to provide sufficient grounds for a refusal to comply with a request.

187. Under the Data Protection Act 1998, individuals had the right to access any of their personal data held by third parties on payment of a nominal fee, set at a maximum of £10, provided the request satisfied certain requirements.[44] With the introduction of the EU GDPR, the charging of a nominal

[41] UK GDPR Article 15

[42] See part 31 of the Civil Procedure Rules which govern the rules of disclosure and inspection of documents in Civil Court proceedings

[43] UK GDPR Article 12(5)(b) and please see ICO guidance: 'When can we refuse to comply with a request?'

[44] Section 7(2) Data Protection 1998 Act (now superseded by the Data Protection Act 2018) See also the Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000 No.191 and 2001 No.3223

fee for responding to subject access requests was no longer permitted in the majority of circumstances.[45] Controllers may refuse compliance with a subject access request or charge a reasonable fee only if the request is either 'manifestly unfounded' or 'manifestly excessive'.[46] However, the ICO has indicated that organisations do not commonly rely on this provision in order to justify a refusal to comply with a request or to charge a fee for compliance.

188. **To address the issues outlined above, the government is considering whether to introduce a fee regime (similar to that in the Freedom of Information Act 2000, which provides for access to information held by public bodies) for access to personal data held by all data controllers (not just public bodies).** The fee regime would be structured so as not to undermine an individual's right to access their personal data. The government recognises that this proposal may impact persons less able to express themselves due to age or disability by resulting in their requests being erroneously treated as 'disproportionate' or 'vexatious' but this may be mitigated by the fact that a third party can raise a subject access request on their behalf. The government is also keen to gather views on whether there is a need for a safeguard similar to the one provided under Section 16 of the Freedom of Information Act in order to help data subjects by providing advice and assistance to anyone who has made, or is thinking of making, a request.

189. This proposal could help to ensure that organisations are not overburdened by wide-ranging, speculative subject access requests. Introducing a fee regime similar to that in the Freedom of Information Act 2000 would address current concerns by:

    a. Introducing a cost ceiling to address organisations' capacity constraints: the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 set a cost limit to prevent organisations being overburdened by requests under the Freedom of Information Act. The regulations define the appropriate cost limit as £600 for central government and £450 for public bodies outside central government, such as local authorities. Only a limited number of tasks count towards this cost and therefore it does not reflect an organisation's actual cost of compliance with each request. This regime gives public bodies the option of either refusing to deal with the request or charging a fee for responding.[47] It is worth noting that there is already a fee charging regime in place for public bodies in relation to subject access requests relating to unstructured manual data.[48] If a similar fee regime were introduced for all subject access requests, organisations (both public and non-public) would still be obliged to deal with the request to the extent possible within the cost limit - for example, by suggesting to the individual the information they may be able to search for, retrieve or extract within the cost limit. The cost limit would not function as a ground on which to refuse outright to deal with a request.

[45] UK GDPR Article 12 (5) 'Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge'.
[46] UK GDPR Article 12: To determine whether a SAR is 'manifestly excessive' an organisation should consider whether the request is proportionate when balanced with the burden or costs involved in dealing with the request. In addition, Data Controllers may also need to consider the different exemptions detailed in Schedules 2-4 of the Data Protection Act 2018. These add to and complement a number of exceptions already built into certain UK GDPR's provisions. Further guidance is available on the ICO website: 'ICO guide to GDPR: Exemptions'
[47] Section 13(1)-(3) Freedom of Information Act 2000 sets out additional fees that may be charged when the cost of compliance exceeds the appropriate limit.
[48] See para 13 of Schedule 20 to the Data protection Act 2018 which sets the appropriate maximum limit of fee regulations for manual unstructured data held by Freedom of Information public authorities (until the regulations under Section 24(8) of the Data protection Act come into force)

b. Amending the threshold for response: the Freedom of Information Act 2000 provides that public bodies may refuse part or the entirety of a freedom of information request, if the request is vexatious.[49] The key test for vexatious requests is whether the request is likely to 'cause a disproportionate or unjustifiable level of distress, disruption or irritation'.[50] When assessing whether a request is vexatious, the ICO's guidance makes clear that the Act permits an organisation to take into account the context and history of a request, including the identity of the requester and any previous contact with them. Applying similar provisions to subject access requests, in place of the thresholds described in paragraph 186 above, would help to prevent organisations needing to respond to subject access requests where access to personal data or concerns about its processing are not the purpose of the request.

The government welcomes views on the following questions:

Q2.3.1. Please share your views on the extent to which organisations find subject access requests time-consuming or costly to process.

Please provide supporting evidence where possible, including:

- *What characteristics of the subject access requests might generate or elevate costs*
- *Whether vexatious subject access requests and/or repeat subject access requests from the same requester play a role*
- *Whether it is clear what kind of information does and does not fall within scope when responding to a subject access request*

Q2.3.2. To what extent do you agree with the following statement: 'The 'manifestly unfounded' threshold to refuse a subject access request is too high'?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, providing supporting evidence where possible, including on what, if any, measures would make it easier to assess an appropriate threshold.

Q2.3.3. To what extent do you agree that introducing a cost limit and amending the threshold for response, akin to the Freedom of Information regime (detailed in the section on subject access requests), would help to alleviate potential costs (time and resource) in responding to these requests?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

[49] Freedom of Information Act 2000, Section 14(1)

[50] ICO website guidance: 'When can we refuse a request as vexatious?'

Please explain your answer, and provide supporting evidence where possible, including on:

- *Which safeguards should apply (such as mirroring Section 16 of the Freedom of Information Act (for public bodies) to help data subjects by providing advice and assistance to avoid discrimination)*
- *What a reasonable cost limit would look like, and whether a different (ie. sliding scale) threshold depending on the size (based on number of employees and/or turnover, for example) would be advantageous*

Q2.3.4. To what extent do you agree with the following statement:'There is a case for re-introducing a small nominal fee for processing subject access requests (akin to the approach in the Data Protection Act 1998)'?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible, including what a reasonable level of the fee would be, and which safeguards should apply.

Q2.3.5. Are there any alternative options you would consider to reduce the costs and time taken to respond to subject access requests?

- *Yes*
- *No*
- *Don't know*

Please explain your answer, and provide supporting evidence where possible.

2.4 Privacy and electronic communications

190. Most of the proposals in this consultation focus on improvements to the UK GDPR and the Data Protection Act 2018, but in some circumstances the processing of personal data is also governed by the Privacy and Electronic Communications Regulations 2003 (PECR).

191. PECR complements the UK GDPR and Data Protection Act 2018 and sets out more specific privacy rights on:

    a. Marketing by electronic means, including marketing calls, texts, emails and faxes

    b. Confidentiality of terminal equipment - for example, computers, mobile phones, wearable technology, smart TVs and connected devices - including the use of cookies or similar technologies that track information about people accessing a website or other electronic services

c. Security of public electronic communications services[51]

d. Privacy of customers using communications networks[52] or services as regards traffic[53] and location[54] data, itemised billing, line identification services - for example, caller ID and call return - and directory listings

192. This means, for example, an organisation that sends a person electronic marketing or places a tracking cookie on their computer must comply with the rules of both PECR and the UK's general data protection regime. Some aspects of PECR apply even if an organisation is not processing personal data because many of the rules protect companies as well as individuals.

193. PECR was created in recognition of the fact that widespread public access to digital mobile networks and the internet opened up new possibilities for businesses and users, but also brought new risks to their privacy. Since its introduction in 2003, our lives have become increasingly digitised and it is important that PECR is reviewed. The aspects of the Regulations that are of particular interest here are the rules on the use of cookies, direct marketing and nuisance calls. The government would therefore welcome views on the following proposals.

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

194. PECR sets out specific rules (Regulation 6) on the confidentiality of terminal equipment such as computers, mobile phones, wearable technology, smart TVs and connected devices, including the Internet of Things.[55] It prohibits an organisation from storing information or gaining access to information stored in the terminal equipment of an individual, unless the individual has provided consent or a narrow range of exemptions apply.

195. These rules apply to the placement of cookies on a person's terminal equipment, as well as other technologies such as machine telemetry, software updates, and ad-ware.[56,57,58] A cookie is a small file stored on a user's terminal equipment by the web browser. Cookies and similar

[51] A public electronic communications service is any service that members of the public can sign up to in order to send or receive electronic signals (including sounds, images or data of any description) – for example, a phone contract or internet connection.It does not include a 'content service' such as a broadcast service or an online news service.
[52] A public electronic communications network is any transmitter or transmission system (plus associated equipment, software and stored data) used to convey electronic signals. This could be a wired or a wireless network – for example, a network of phone cables or a mobile phone network.
[53] Traffic data includes information about the routing, duration or timing of any phone call, text or email, whether it relates to an individual or a company.
[54] Location data is information collected by a network or service about where the user's phone or other device is or was located. The Geospatial Commission (part of the Cabinet Office) is undertaking a Public Dialogue to gather evidence on public perceptions on the responsible use of location data in support of a UK Geospatial Strategy commitment to publish guidance on the ethical use of location data.
[55] The Privacy and Electronic Communications (EC Directive) Regulations 2003, UK Statutory Instruments 2003, No. 2426, Regulation 6
[56] Machine telemetry is the in situ collection and automatic transmission of measurements or other data concerning the machine.
[57] A software update means a modification to the software product that corrects errors including maintenance-only releases, bug fixes, and patch-kits.
[58] Software that automatically puts advertisements onto a computer screen when a person is using the internet.

technologies such as web beacons and device fingerprinting can be used to collect different types of data for a range of different purposes.[59,60] For example:

a. 'Strictly necessary': cookies can be essential to make a website work properly, such as authentication cookies which allow a person to use the same username and password to access a particular site, or cookies that are used to remember what a user has added to their shopping basket during a browsing session. Consent is not required to place these types of cookies as they are strictly necessary for the delivery of the services requested by the user.

b. Analytics: cookies are used so that online services can collect information about how people access them – for example, the number of users on a website, how long they stay on the site for, and what parts of the site they visit. This is also sometimes known as 'web audience measurement'. Such cookies often collect information that is anonymous, or present low risk to privacy. Currently consent is required to place these types of cookies on the user's device.

c. Tracking: cookies may also collect, use or share data about a particular user's activity across multiple distinct sites, creating profiles for use - for example, in online advertising. Privacy concerns tend to arise in relation to cookies that collect a large and diverse set of data, which are more invasive.[61] Consent is required to place these types of cookies on the user's device.

Case study: *Cross-property tracking for personalised advertising purposes*

The aim of cross-property tracking is to link together the activity of a single user across different sessions, properties (web pages and apps) and devices in order to build a more complete profile of that individual. This profile can then be used to help deliver personalised advertising and inform spending decisions of advertisers.

Personalised advertising requires knowledge about an individual in order to determine whether to show them any ads, which ads to show them, and to measure the individual's response. The profile of an individual may consist of volunteered or inferred data on demographic information or interests, as well as past browsing and purchasing behaviour. This is different to contextual advertising, which relies on information about the content and context of the web page or app that the individual is viewing.

Most digital advertising is sold using automated systems and processes to buy and sell inventory in real time - this is known as real time bidding. When a user visits a web page or app with an ad space, the publisher may send a request for bids from advertisers to fill that space. Most bid requests will contain pieces of personal data, which can be used to identify the user and information on the webpage URL or app that the user is viewing. This may even include contextual information that could support inferences about health, sexuality, politics, religion, or ethnicity. Bid requests are sent to potentially hundreds of adtech intermediaries and advertisers. Real-time bidding takes milliseconds from the collection of

[59] Web Beacon also known as a web bug, pixel tag or clear GIF. The web beacon operates as a tag that records an end user's visit to a particular web page or viewing of a particular email. It is also often used in conjunction with a web cookie and provided as part of a third-party tracking service.
[60] Device fingerprinting is a technique used to identify a user's device based on its unique configuration.
[61] ICO 'Update report into adtech and real time bidding', 20 June 2019.

the user's information through to the presentation of the advert to the individual.

196. Under the current legislation, organisations are not permitted to place cookies on websites, or other technology without the consent of the individual, unless they are 'strictly necessary' for delivering an online service.[62] This requirement is not risk-based and is interpreted very narrowly, which means that consent is necessary for even low risk activities, such as the use of analytics cookies. Consent will usually be sought via pop-up notifications when a user visits a website or accesses a service.

197. This has resulted in two issues:

    a. Organisations' ability to collect audience measurement data in order to improve their websites and services for their customers has been affected by the stricter consent requirements that are intended to give consumers greater control over how their data is used

    b. Individuals frequently complain about the number of cookie pop-ups on websites. There is evidence to suggest that many people do not engage with privacy information and controls, and simply accept the terms or use of cookies because they want to access the website.[63] The use of nudge techniques may encourage users to provide consent or turn off privacy protections[64,65]

198. **The government is considering two main options for tackling these issues. The first option would permit organisations to use analytics cookies and similar technologies without the user's consent.** In effect, these cookies would be treated in the same way as 'strictly necessary' cookies under the current legislation for which consent is not required. However, further safeguards may need to be considered to ensure that such processing poses a low impact on users' privacy and a low risk of harm. This option would not remove the requirement on organisations to provide the user with clear and comprehensive information about the measurement technologies that are active on their device and the purposes behind the use of the technology.

199. Other countries, such as France, already view analytics (or 'audience measurement') cookies as being 'strictly necessary' and therefore do not require consent when certain conditions are met, for example:

    a. The scope of use is limited to a single website or application, and cannot be used to track individuals across applications or websites

    b. The purpose must be limited to analysing website performance or similar purposes

[62] The meaning of consent in PECR was brought in line with its meaning in the UK GDPR, which means that a person must be given the opportunity to give clear, purposeful consent to the use of cookies which are not strictly necessary.
[63] Deloitte: 'Digital Consumer Trends', 2020.
[64] Nudge techniques are design features which lead or encourage users to follow the designer's preferred paths in the user's decision making. For example, the use of a large prominent 'yes' button next to a smaller print 'no' option, with the result that the user is 'nudged' towards answering 'yes' rather than 'no' to whatever option is being presented.
[65] CMA: 'Online platforms and digital advertising market study', 2019.

c. The use of data collected must be limited to the production of statistical reports using aggregated or otherwise anonymised data (for example, 30% of users leave a site in under two minutes) and not reporting on individual behaviours (for example, a specific user has shown a particular interest in this section of the site, therefore it is possible to infer some of their likely preferences)

200. **The government also welcomes evidence on the risks and benefits of a second option, which could permit organisations to store information on, or collect information from, a user's device without their consent for other limited purposes.** This could include processing that is necessary for the legitimate interests of the data controllers where the impact on the privacy of the individual is likely to be minimal - such as when detecting technical faults or enabling use of video or other enhanced functionality on websites. Arguably service users might reasonably expect a data controller to carry out such activities without their consent and this proposal would bring this aspect of PECR closer into line with the legitimate interests lawful basis under the UK GDPR (see section 1.4 of this consultation for more information on how that basis works in practice).

201. As in the first option above, the purposes of the processing would need to be carefully explained. Any list of exceptions to the consent requirement would need to be kept up to date in order to respond to technological advancements. Additional safeguards could also be explored, as appropriate, such as: the use of pseudonymisation; mandating that information is not used to build a profile of the user; or requiring the use of transparency notices. The government is also interested to hear views on how sectoral codes (see Article 40 of the UK GDPR) or regulatory guidance could provide a flexible means of balancing the safeguarding of users' privacy with technical and service innovation.[66]

202. The government recognises that users value privacy and want control over how their personal data is used.[67] These options would not permit organisations to use data in privacy-intrusive ways without the consent of the individual - for example, for invasive tracking purposes, micro-targeting and real-time bidding, which involves sharing information about the user with third party advertisers. Organisations would also need to continue to comply with other relevant legislation, such as the UK GDPR, and regulatory guidance, such as the ICO's Age Appropriate Design Code, so that information notices and procedures for consent are valid and suitable for different users, including children and people in other vulnerable groups.

203. These options will not entirely remove consent pop-ups, especially as many organisations based overseas will continue to comply with different regulations. But, where controllers comply with any new provisions under UK legislation, it may mean consumers can direct more of their time and attention to making important decisions about the use of cookies and other technology that may have a material effect on their privacy.

204. The overall impact of the options outlined above could be enhanced if users can express their privacy preferences through browsers, software applications and device settings. This would potentially remove the need for consent pop-up notices on each website or service. The government can see the benefits of allowing an individual to express their privacy preferences on a single occasion and to have control over how these preferences are applied. These solutions often rely, however, on services provided by large companies in digital markets. The government is aware of Apple Inc's and Google's separate approaches to the use of third-party cookies. This

[66] ICO 'Codes of Conduct'.

[67] CMA, 'Online platforms and digital advertising market study', 2019

approach may not necessarily provide a complete solution if it risks strengthening some market players' access to data.

205. Any approach should support a dynamic and competitive sector so that people using online services can benefit from choice, fair prices and secure data. The Information Commissioner and the Competition and Markets Authority are working together to promote digital markets which are competitive, empower consumers and safeguard individuals' data protection rights.

206. **The government recognises there may be alternatives to web browser solutions or software applications that achieve the effect of removing cookie pop-up notices altogether.** The Taskforce on Innovation, Growth and Regulatory Reform has suggested that data fiduciaries or other trusted third parties could play a role in managing an individual's consent preferences.[68] Such a system could potentially put an end to cookie pop-up notices directed at individual users. An alternative approach is the removal of the requirement for prior consent for all types of cookies, irrespective of whether individuals have set their preferences via web browser technologies or through trusted data fiduciaries. Although this would make compliance with PECR more straightforward for organisations, they would continue to be required to comply with UK GDPR principles on lawfulness, fairness and transparency when using cookies or similar technologies. The government would welcome views on how organisations could comply with these principles without the use of cookie pop-up notices.

The government welcomes views on the following questions:

Q2.4.1. What types of data collection or other processing activities by cookies and other similar technologies should fall under the definition of 'analytics'?

Q2.4.2 To what extent do you agree with the proposal to remove the consent requirement for analytics cookies and other similar technologies covered by Regulation 6 of PECR?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your choice, and provide supporting evidence where possible, including what safeguards should apply.

Q2.4.3. To what extent do you agree with what the government is considering in relation to removing consent requirements in a wider range of circumstances? Such circumstances might include, for example, those in which the controller can demonstrate a legitimate interest for processing the data, such as for the purposes of detecting technical faults or enabling use of video or other enhanced functionality on websites.

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*

[68] Proposal 7.1 of the Taskforce on Innovation, Growth, and Regulatory Reform report, May 2021.

- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible, including what circumstances should be in scope and what, if any, further safeguards should apply.

Q2.4.4. To what extent do you agree that the requirement for prior consent should be removed for all types of cookies?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible, including how organisations could comply with the UK GDPR principles on lawfulness, fairness and transparency if PECR requirements for consent to all cookies were removed.

Q2.4.5. Could sectoral codes (see Article 40 of the UK GDPR) or regulatory guidance be helpful in setting out the circumstances in which information can be accessed on, or saved to a user's terminal equipment?

Q2.4.6. What are the benefits and risks of requiring websites or services to respect preferences with respect to consent set by individuals through their browser, software applications, or device settings?

Q2.4.7. How could technological solutions, such as browser technology, help to reduce the volume of cookie banners in the future?

Q2.4.8. What, if any, other measures would help solve the issues outlined in this section?

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

207. PECR also regulates the use of electronic messages (such as emails, texts and video messages) for direct marketing purposes. Direct marketing covers the promotion of aims and ideals as well as the sale of products and services.

208. Currently businesses may generally only contact individuals who have previously been in touch during a sale or transaction, and have not refused or opted out of receiving marketing communications about similar products. This is known as a 'soft opt-in'. These provisions strike a balance between preserving people's data protection rights and allowing legitimate business activities.

209. However, the soft opt-in is currently only available to commercial organisations; there is no equivalent provision for non-commercial organisations which engage in direct marketing - for example, charities and political parties (section 2.5 below discusses the use of personal data for the purposes of democratic engagement in more detail).

210. **The government proposes to extend the soft opt-in to electronic communications from organisations other than businesses where they have previously formed a relationship with the person, perhaps as a result of membership or subscription.**

211. Organisations relying on the soft opt-in must give a person the chance to opt out when they first collect the person's contact details and in every subsequent communication they send. It must also be simple to opt-out - for example a person should be able to reply directly to an email message, or click a clear 'unsubscribe' link.

The government welcomes views on the following questions:

Q2.4.9. To what extent do you agree that the soft opt-in should be extended to non-commercial organisations? See paragraph 208 for description of the soft opt-in.

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Nuisance and fraudulent calls

212. PECR already prohibits organisations that undertake direct marketing from contacting individuals by phone if they are registered with the Telephone Preference Service or have previously informed the company that they do not wish to be contacted. Over the last few years, the government has made a number of changes to PECR to provide consumers with greater protection from unsolicited direct marketing ('nuisance') calls. For example, it introduced director liability in 2017 to prevent rogue directors liquidating their companies in order to avoid paying fines. More recently, it has banned cold calls from pension providers and claims management firms, unless individuals have expressly agreed to be contacted.

213. The legislation has led to enforcement action against a number of UK-based firms responsible for unsolicited marketing calls and texts, but communications from overseas are harder to tackle.[69] Unsolicited direct marketing calls do not usually amount to criminal conduct and not all companies that make them are aiming to scam or defraud consumers. However, these calls may still cause anxiety or frustration for many people and possibly lead to significant distress for the most vulnerable people in society.

214. As well as unsolicited calls, many people report receiving other forms of electronic communications, such as text messages and emails, which appear to be from criminals seeking

[69] ICO website, 'Actions we've taken', 'Enforcement action'

to defraud them.[70,71] During the COVID-19 pandemic, for example, there were several reports of people receiving fraudulent calls encouraging them to pay a fee for vaccines that were free on the NHS. Other scams have been reported whereby fraudsters 'spoof' the telephone numbers of legitimate businesses to convince people to part with bank details or other financial information.

215. The government is working closely with telecommunications providers, regulators, law enforcement agencies and consumer groups to develop and progress strategies to counter the rising number of fraudulent communications. A voluntary charter for telecommunications providers is currently in development on actions they can take to prevent fraud. Earlier this year, the Home Secretary chaired the Economic Crime Strategic Board, which agreed a framework to develop a Fraud Action Plan that will include prevention, education, effective enforcement and regulatory reforms across several industries, including the telecommunications sector.

The government welcomes views on the following questions:

Q2.4.10. What are the benefits and risks of updating the ICO's enforcement powers so that they can take action against organisations for the number of unsolicited direct marketing calls 'sent'?

Currently the ICO can only take action on calls which are 'received' and connected. The ICO sometimes receives intelligence of companies sending thousands of calls but which are not all connected, but they cannot take account of the potential risk of harm when determining the most appropriate form of enforcement action.

Q2.4.11. What are the benefits and risks of introducing a 'duty to report' on communication service providers?

This duty would require communication service providers to inform the ICO when they have identified suspicious traffic transiting their networks. Currently the ICO has to rely on receiving complaints from users before they can request relevant information from communication service providers.

Please provide information on potential cost implications for the telecoms sector of any new reporting requirements.

Q2.4.12. What, if any, other measures would help to reduce the number of unsolicited direct marketing calls and text messages and fraudulent calls and text messages?

Q2.4.13. Do you see a case for legislative measures to combat nuisance calls and text messages?

- *Yes*

[70] ICO, 'Nuisance calls and messages, Update to ICO / Ofcom joint action plan', 23 March 2021

[71] In April 2020, the National Cyber Security Centre (NCSC) launched a Suspicious Email Reporting Service. As of 31st May 2021 the number of reports received stood at more than 6,100,000 with the removal of more than 45,000 scams and 90,000 URLs.

- *No*
- *Don't know*

If yes, what measures do you propose and why?

If no, please explain your answer, and provide supporting evidence where possible.

Q2.4.14. What are the benefits and risks of mandating communications providers to do more to block calls and text messages at source?

Q2.4.15 What are the benefits and risks of providing free of charge services that block, where technically feasible, incoming calls from numbers not on an 'allow list'? An 'allow list' is a list of approved numbers that a phone will only accept incoming calls from.

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

216. The Information Commissioner already has powers to take action against breaches of PECR. For example, the Information Commissioner can serve a monetary penalty notice of up to £500,000, which can be issued against the organisation or its directors. This is significantly lower than the fines that the Information Commissioner can impose under the UK GDPR, however. Under that legislation, the Commissioner can issue a fine of up to £17.5 million or 4% global turnover depending upon the contravention of the UK GDPR.

217. Increasing the fines that can be imposed under PECR to the same level as the UK GDPR could help to ensure that the enforcement regime is dissuasive, particularly when addressing serious infringements of PECR. The ICO has imposed the maximum fine available under PECR. In 2020, the ICO issued an enforcement notice against a company which instigated 193,606,544 attempted automated calls, of which 63,615,075 connected, between 1 June and 1 October 2018.

218. The current regime is also less flexible in terms of the investigatory tools available to the Information Commissioner - for example, there is no assessment notice power available under PECR. An assessment notice allows the ICO to consider whether an organisation is compliant with the legislation. It may, for example, require an organisation to give the ICO access to premises and specified documentation and equipment. The government is interested in views on the effectiveness of PECR's enforcement regime.

The government welcomes views on the following questions:

Q2.4.16. To what extent do you agree with increasing fines that can be imposed under PECR so they are the same level as fines imposed under the UK GDPR (i.e. increasing the monetary penalty maximum from £500,000 to up to £17.5 million or 4% global turnover, whichever is higher)?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*

- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q2.4.17. To what extent do you agree with allowing the ICO to impose assessment notices on organisations suspected of infringements of PECR to allow them to carry out audits of the organisation's processing activities?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q2.4.18. Are there any other measures that would help to ensure that PECR's enforcement regime is effective, proportionate and dissuasive?

- *Yes*
- *No*
- *Don't know*

If yes, what measures do you propose and why?

2.5 Use of personal data for the purposes of democratic engagement

219. The government has worked tirelessly to build our democratic system and values, and the safeguarding and integrity of our democratic processes is an absolute priority. There is a collective responsibility on all those in public life to promote democratic engagement, such as local councils, political parties, and civil society groups.

220. In recognition of the importance of a flourishing democracy, the government is keen to understand how the UK GDPR and PECR can continue to support democratic engagement by political parties and elected representatives, whilst ensuring public confidence and trust in how their personal data is used.

221. The government would welcome views on two main issues: i) whether communications from political parties which promote aims and ideals should continue to be treated as direct marketing for the purposes of PECR; and ii) whether the lawful grounds for processing personal data, including personal data revealing political opinions, under Articles 6 and 9 of the UK GDPR permit political parties and elected representatives to process personal data for the purposes of democratic engagement to the extent that is necessary in a healthy democracy.

<u>Political campaigning and direct marketing rules under PECR</u>

222. Case law has established that communications from political parties which promote aims and ideals should be classified as direct marketing for the purposes of PECR.[72] In other words, political parties should not call, email or text prospective voters for purposes such as campaigning or fundraising, unless they have obtained prior consent. This position is reflected in the ICO's guidance on political campaigning and direct marketing, but it has never been fully debated in the UK Parliament.[73] The government would welcome views on whether electronic communications from political parties and other political entities, such as candidates and third-party campaign groups registered with the Electoral Commission, for campaigning purposes should continue to be subject to exactly the same rules as communications from commercial organisations in connection with goods and services. Relaxing the rules could give organisations more freedom to engage with prospective voters without their consent and may help to increase voter turnout at election time. On the other hand, the government recognises that people may not wish to receive electronic communications from political parties or elected representatives much in the same way as they would not wish to receive commercial marketing material. For example, some people may not agree with allowing robo-calls (automated telephone calls which deliver a recorded message) to be used for campaigning purposes without the consent of the prospective voter.

223. The government considers that if communications for the purposes of democratic engagement are to continue to be subject to PECR as a form of direct marketing, organisations which send them should be able to rely on the 'soft opt-in' provisions which are already available to commercial organisations (see section 2.4 above). This would allow political parties to communicate with voters who had previously shown an interest in the party, perhaps through membership or attendance at a conference, without seeking their express consent.

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

224. Section 8 of the Data Protection Act 2018 makes clear that processing personal data for democratic engagement falls within the 'public interests tasks' lawful ground in Article 6(1)(e) of the UK GDPR. In order to rely on this lawful ground, however, Article 6(3) of the UK GDPR provides that organisations must also identify a separate legal basis elsewhere in the law which explains the nature and purposes of the processing. This is an important safeguard for data subjects because it prevents any data controller processing personal data without consent by claiming to be carrying out a task in the public interest.

225. For example, electoral legislation permits political parties, electoral candidates and elected officials to access data from the electoral register for the electoral purposes, such as political campaigning.[74] This allows for the data to be used in pursuit of legitimate public aims in a transparent manner that is proportionate to the intrusion into individual privacy. Since it is not possible for a citizen to 'opt out' from these uses of data from the electoral register, any expansion of its uses, including allowing the data to be combined in unforeseen ways with other personal data, could deter the public from registering to vote, therefore driving down engagement and negatively impacting the completeness of the electoral register. We intend to legislate to

[72] Scottish National Party v Information Commissioner (EA/2005/0021, 15 May 2006)

[73] Section 122(5) of the Data Protection Act 2018 provides that "direct marketing" means the communication (by whatever means) of advertising or marketing material which is directed to particular individuals, but there was no extensive debate on these provisions.

[74] See e.g. (for England & Wales) regulations 103-105 of The Representation of the People (England and Wales) Regulations 2001 as inserted by regulation 15 of The Representation of the People (England and Wales) (Amendment) Regulations 2002.

align the terminology used across electoral and data law to provide greater clarity for data users and subjects alike.

226. Beyond this, the government understands that some parties and elected representatives have not always been able to identify a clear legal basis for processing personal data from other sources. This would not necessarily prevent processing of that data, as parties could potentially rely on alternative lawful bases in Article 6 (such as processing which is necessary for the legitimate interests of the data controller), but the government would welcome evidence from political parties and elected representatives about whether there are any barriers created by the current framework and, if there are, ideas for possible solutions.

227. When organisations are processing sensitive data, which includes personal data revealing political opinions, they must identify a relevant provision under Article 9 of the UK GDPR as supplemented by Schedule 1 to the DPA 2018, as well as a lawful ground for processing under Article 6. Paragraph 22 of Schedule 1 to the DPA 2018 permits registered political parties to process sensitive data about people's political opinions without consent where it is necessary for the purposes of their organisation's political activities and provided that the processing does not cause damage or distress. For the purposes of this provision, political activities are said to include campaigning, fund-raising, political surveys and case-work. Paragraph 23 of the same Schedule permits elected representatives to process sensitive data without consent where they have been requested to act on behalf of a constituent and the processing is carried out in connection with the discharge of their functions.

228. The government would welcome views, particularly from political parties and elected representatives, on whether the provisions in Schedule 1 to the DPA 2018 are working as they should or whether there are aspects of these provisions that could be improved to support the use of data for the purposes of democratic engagement.

The government welcomes views on the following questions:

Q2.5.1. To what extent do you think that communications sent for political campaigning purposes by registered parties should be covered by PECR's rules on direct marketing, given the importance of democratic engagement to a healthy democracy?

Please explain your answer, and provide supporting evidence where possible.

Q2.5.2. If you think political campaigning purposes should be covered by direct marketing rules, to what extent do you agree with the proposal to extend the soft opt-in to communications from political parties?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q2.5.3. To what extent do you agree that the soft opt-in should be extended to other political entities, such as candidates and third-party campaign groups registered with the Electoral Commission? See paragraph 208 for description of the soft opt-in

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q2.5.4. To what extent do you think the lawful grounds under Article 6 of the UK GDPR impede the use of personal data for the purposes of democratic engagement?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q2.5.5 To what extent do you think the provisions in paragraphs 22 and 23 of Schedule 1 to the DPA 2018 impede the use of sensitive data by political parties or elected representatives where necessary for the purposes of democratic engagement?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

2.6 Further Questions

Q2.6.1. In your view, which, if any, of the proposals in 'Reducing burdens on business and delivering better outcomes for people', would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

Q2.6.2. In addition to any of the reforms already proposed in 'Reducing burdens on business and delivering better outcomes for people', (or elsewhere in the consultation), what reforms do you think would be helpful to reduce burdens on businesses and deliver better outcomes for people?

Chapter 3 - Boosting trade and reducing barriers to data flows

3.1 Introduction

229. Global networks of data flows are critical to our prosperity and modern way of life. Consumers and businesses collect, share and process personal data internationally in order to use or trade digital products and services. According to the World Trade Organization, trade in data-enabled services grew from $1.0 trillion in 2005 to $2.4 trillion in 2017.[75] Data flows have a larger impact in raising world GDP than the trade in goods.[76] In 2019 the UK exported £234 billion in data-enabled services (74% of total UK services exports) and imported £124 billion in data-enabled services (57% of total UK services imports).[77]

230. The government intends to facilitate digital trade and influence the global rules that govern the cross-border flow of goods, services and data. It is committed to working with international partners to remove unnecessary barriers to cross-border data flows, including by agreeing to commitments in bilateral and plurilateral trade agreements, through negotiations at the World Trade Organisation, and by driving forward data free flow under the UK's G7 presidency.

231. The government's ambition is for the UK to be a leader in digital trade and the world's most attractive data marketplace: an open, welcoming and secure destination for companies from all over the world to share data, grow their businesses and innovate across all sectors of the economy. This includes giving people the confidence that their personal data will be protected when it is in the UK and when it is transferred overseas. In the UK's free trade agreements, provisions facilitating trusted cross-border data flows go hand in hand with the UK's high standards of data protection. For example, our ambition for Personal Information Protection provisions in free trade agreements promotes high standards across parties, supporting compatibility with other countries' domestic data protection frameworks.

232. International data flows also play an important role in the UK's efforts to ensure and improve public safety. Enhancing public safety remains a central objective and the government is committed to strengthening its ability to protect its citizens through intensified cooperation with international law enforcement partners. It is vital that the UK can capitalise on the benefits of global data sharing and efficiently safeguard the public at the same time. Greater law enforcement cooperation will provide the UK with increased capabilities to achieve public safety aims.

233. The government aims to create an autonomous UK framework of international data transfers that reflects the UK's independent approach to data protection, and supports its wider objectives for trade and security. There is an opportunity to explore more flexible, innovative and reliable mechanisms for protecting personal data when it is transferred overseas. As set out in this chapter, this includes more effectively using the UK's data adequacy framework, which empowers the government to recognise that data protection standards in another jurisdiction are high enough to remove the need for additional safeguards, and improving the alternative tools that facilitate protected personal data flows. This will help domestic businesses to connect more

[75] World Trade Report 2019: The Future of Services Trade, *Figure D.6: Global exports of ICT-enabled services*
[76] McKinsey 2016, Digital Globalization: The New Era of Global Flows
[77] DCMS, 'Understanding and measuring cross-border digital trade Final Research Report', 14th May 2020

easily with foreign markets, while attracting investment from abroad by businesses that rightly have confidence in the responsible use of data within the UK.

3.2 Adequacy

234. Having left the European Union, the UK can capitalise on its independent status and repatriated powers in pursuit of the data opportunity. This includes having the freedom to strike our own international data partnerships with some of the world's fastest growing economies, using our data adequacy capability.

Explanatory box: *What is a data adequacy capability?*

Under UK law, there are general restrictions on transferring personal data to other countries, in order to ensure that people's data is sufficiently protected. Personal data can only be transferred to another country if that country provides an adequate level of protection, if there are appropriate safeguards in place to protect the personal data, or if one of a limited number of exceptions applies.

UK law allows the government to assess whether other countries' laws and practices provide an 'adequate' level of personal data protection. Where this assessment finds that a country does provide an adequate level of personal data protection, data adequacy status is granted to that country. Data adequacy findings are given effect through adequacy regulations made by the government. The effect of adequacy regulations is that personal data can be sent from the UK to the adequate country without any requirement for further safeguards. In practice, this means that a UK-based organisation can send personal data to an organisation based in the adequate country without needing to put in place additional measures (such as standard contractual clauses) to ensure that the data is protected.

Adequacy regulations made by the government provide greater certainty and confidence in other countries' data protection regimes.

235. The government is committed to the reduction of barriers and burdens that organisations face when transferring personal data freely and safely overseas. When assessing the data protection standards in other countries for adequacy, its ambition is to take a creative, collaborative and pragmatic approach and ensure high standards of data protection.

236. Under UK law there are two types of adequacy regulations: one which covers general data processing under the UK GDPR and Part 2 of the Data Protection Act 2018 and one which covers law enforcement data processing under Part 3 of the Data Protection Act 2018. The approach discussed in this section applies to both types of adequacy regulations.

237. Currently UK law treats as adequate for general data processing purposes the European Union and EEA states, the European Union institutions, the 12 countries the European Union had already assessed as adequate prior to European Union exit, and Gibraltar. For law enforcement data processing purposes, UK law treats as adequate the European Union and EEA states, Switzerland and Gibraltar. **The government intends to add more countries to the list by progressing an ambitious programme of adequacy assessments in line with the UK's global ambitions and commitment to high standards of data protection.** Doing so will

provide UK organisations with a simple and safe mechanism for international transfers of personal data.

238. **Finally, the government intends to ensure that all adequacy regulations made under our current laws remain valid under any future regime.** The European Union took a similar approach when it rolled over the validity of all European Union adequacy decisions adopted prior to the GDPR as valid under the GDPR.

A risk-based approach to adequacy regulations

239. The government recognises that organisations currently face challenges and uncertainty when transferring personal data internationally. Overly prescriptive approaches to adequacy cannot recognise the different cultural, legal and linguistic factors that can contribute to high standards of data protection. Such approaches make it unnecessarily inflexible and impractical to transfer data overseas, limiting the benefits that global data sharing can bring if undertaken in a responsible way.

240. Recent legal developments, including the *Schrems II* judgment, have made it more difficult for UK data exporters to transfer personal data overseas (see explanatory box below). The invalidation of the Privacy Shield by this judgment was particularly disruptive given the volume of trade it supported and the very many small and medium-sized businesses that were relying on it.[78] Outside of the European Union, the UK has an opportunity to consider both the impact of this judgment on its transfers regime and how best to support international data flows in the future.

Explanatory box: *Schrems II: Court of Justice of the European Union's judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*

On 16 July 2020, the Court of Justice of the European Union invalidated the European Union's adequacy decision for the EU-US Privacy Shield – a framework that permitted Trans-Atlantic personal data transfers to certified US organisations, including transfers between the UK and the US. The Privacy Shield scheme requires US based organisations to certify to a standard agreed between the US and European Union; organisations must commit to comply with the requirements which are enforceable under US law.

In the same judgment the court upheld the validity of Standard Contractual Clauses - a tool organisations can use to ensure appropriate safeguards are applied to personal data transfers. This was however qualified, and the Court's judgment required organisations to consider whether, in the circumstances of each transfer, the Standard Contractual Clauses do in practice provide an 'essentially equivalent' level of protection for the personal data - and if they do not, to only proceed with the transfer if supplementary measures are adopted alongside the Standard Contractual Clauses sufficient to address the shortfall in safeguards.

The UK Government intervened in the case, arguing in support of the validity of Standard Contractual Clauses. The government subsequently published a statement noting disappointment that the European Union's adequacy decision for the Privacy Shield had been invalidated.

[78] See Schrems II box for more detail on Privacy Shield

241. A majority of respondents to the government's National Data Strategy consultation agreed that the UK can improve on current international data transfer mechanisms by reviewing standards, rules and regulations, and working to reduce unnecessary barriers to cross-border data flows. Furthermore, the UK is well positioned to lead the global debate to strike the right balance on these key issues owing to: its long-standing and enduring commitment to high standards of data protection; its rich and sophisticated data market; its outward-facing and international outlook; its internationally respected regulator for data protection, the ICO; its commitment to pragmatism and risk-based solutions, and; its role as custodians of a world-class national security regime that puts the protection of citizens and individuals' rights at the core.

242. **In light of these developments, the government intends to approach adequacy assessments with a focus on risk-based decision-making and outcomes.** Adequacy assessments should take into account the likelihood and severity of actual risks to data subjects' data protection rights. This approach will account for the actual practices that materially affect international data transfers between the UK and another jurisdiction, rather than accounting for academic or immaterial risks. There may be practices in a particular country that are perceived to undermine data subject rights but if, for example, these practices are not applied in specific sectors or territories, then the risk to data subjects when making an adequacy finding in respect of those specific sectors or territories is very low or immaterial.

243. Furthermore, future adequacy decisions will be based more heavily on an assessment of the real-world outcomes of data protection regimes rather than on a largely textual comparison of another country's legislation with the UK's legislation. This approach will recognise the different legal and cultural traditions which inform *how* other countries achieve high standards of data protection.

244. Adequacy assessments should continue to inspire the trust and confidence of individuals, organisations and international partners. Adequacy assessments will therefore still be based on a robust, technical assessment of relevant data protection laws and practices. They will 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.

245. The government will use a four stage procedure to ensure that UK citizens and consumers can have confidence in the adequacy regulations that are made. These four stages are:

    a. Gatekeeping stage: consideration of whether to commence an adequacy assessment in respect of a country, by reference to policy factors, including high standards of data protection and the UK's strategic interests

    b. Assessment stage: collection and analysis of information relating to the level of data protection in another country; this will look at questions based on key principles of the safeguards in the UK GDPR, while recognising that countries protect personal data in different ways

    c. Recommendation stage: officials will make a recommendation to the Secretary of State for Digital, Culture, Media and Sport, who will, after consulting the Information Commissioner and any others considered appropriate, decide whether to make a determination of adequacy in respect of a specific country

    d. Procedural stage: making relevant regulations - and laying these in Parliament - to give legal effect to an adequacy determination

246. **The UK's approach to adequacy must appropriately account for the duty of governments to keep their citizens safe**. Human rights principles and standards will continue to be crucial to adequacy assessments. These principles recognise that necessary and proportionate interference with privacy rights can be justified in order to protect the public and are compatible with high standards of data protection. When considering the access by other countries' public authorities to personal data during adequacy assessments, the government will take into account principles drawn from relevant laws, such as the European Convention on Human Rights, which has been incorporated into UK law through the Human Rights Act 1998, rather than the EU Charter of Fundamental Rights, which is not retained in UK law after exit from the European Union.

The government welcomes views on the following questions:

Q3.2.1. To what extent do you agree that the UK's future approach to adequacy decisions should be risk-based and focused on outcomes?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer and provide supporting evidence if possible.

Creating a scalable, flexible adequacy regime

247. The UK's adequacy assessments should be forward-looking and compatible with the increasing trend towards multilateral and regional approaches to data protection. This is a global trend with multilateral approaches being adopted from Africa through to the Council of Europe's modernisation of Convention 108.[79] An approach which is pragmatic and flexible will help to connect the UK to the rest of the world wherever high data protection standards are maintained.

248. **With this in mind, the government will consider whether to make adequacy regulations for groups of countries, regions and multilateral frameworks**. A group of countries may share harmonised data protection standards, or may adhere to a multilateral framework that underpins data sharing. The group of countries to which such standards apply would be assessed for adequacy collectively. This process would be accompanied with an assessment of the implementation and enforcement of data protection standards, as well as other relevant laws and practices, at a national level.[80] Adequacy could therefore be awarded to a group of countries that have a shared, harmonised, or common framework.

249. Adequacy is increasingly seen as a living mechanism; it should be adaptable to evolving business and legal realities through the review of relevant developments. Such reviews can help to ensure the durability of adequacy regulations. At present, the Secretary of State for Digital, Culture, Media and Sport is under a duty to monitor, on an ongoing basis, any significant developments in an adequate country and to review adequacy regulations at periodic intervals of no longer than four years. Periodic reviews risk imposing an unnecessarily artificial deadline, not least given the duty to monitor on an ongoing basis. This risk increases as the list of adequate

[79] For example, the African Union Convention on Cyber Security and Personal Data Protection.
[80] Art 45(2)(a) of UK GDPR lists factors to be considered, many of these are only appropriate at national level.

destinations expands because there will be more countries to monitor and review, which might affect the UK's ability to prioritise its activities to keep pace with global developments, make new adequacy regulations and review any decisions, as necessary, on the basis of risk.

250. **The government intends therefore to relax the requirement to review adequacy regulations every four years**. The priority will instead be investment in ongoing monitoring of countries' relevant laws and practices, which will help to ensure more efficiently that third countries continue to provide adequate standards of data protection.

The government welcomes views on the following questions:

Q3.2.2. To what extent do you agree that the government should consider making adequacy regulations for groups of countries, regions and multilateral frameworks?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q3.2.3. To what extent do you agree with the proposal to strengthen ongoing monitoring of adequacy regulations and relax the requirement to review adequacy regulations every four years?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Redress requirements

251. Redress mechanisms ensure that there is proper accountability for the provision of necessary protections for data subjects and a means of addressing any shortcomings when personal data is transferred overseas. If data subjects' rights are infringed, redress can provide compensation, other forms of relief or ensure enforcement. The redress that data subjects can benefit from will depend on the laws in the relevant country.

252. The current text of the UK GDPR is not clear about whether the redress that data subjects are entitled to ought to be administrative or judicial. Judicial redress generally refers to a remedy in a court or tribunal, whereas administrative redress could be provided through other means, such as through a national regulator or ombudsperson. In the UK, for example, redress sought through the ICO would be considered administrative.

253. The types of redress available will differ by country. Redress mechanisms available in third countries should be required to be effective and have sufficient power to provide legally binding remedies as appropriate to the circumstances, whether they are judicial or administrative.

254. **To reflect this, the government proposes to amend the legislation to be clear that both administrative and judicial redress are acceptable as long as the redress mechanism is effective**.

The government welcomes views on the following questions:

Q3.2.4. To what extent do you agree that redress requirements for international data transfers may be satisfied by either administrative or judicial redress mechanisms, provided such mechanisms are effective?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your choice, and provide supporting evidence where possible.

3.3 Alternative Transfer Mechanisms

255. Alternative transfer mechanisms provide a route for cross-border transfers of personal data to countries that are not subject to an adequacy decision. Alternative transfer mechanisms are typically agreements which provide binding and enforceable protections for individuals' personal data when it is transferred internationally.

Explanatory box: *What are alternative transfer mechanisms?*

The UK GDPR restricts transfers of personal data to countries outside the UK.

If another country has been assessed as adequate (see text box under section 4.2), organisations may send personal data to recipients in that country without the need for additional safeguards. If the recipient is in a country, territory, or sector which has not been assessed as adequate, organisations must put in place 'appropriate safeguards' in order to make a transfer of personal data.

Article 46 of the UK GDPR provides a range of options for how appropriate safeguards can be provided. These safeguards are commonly known as alternative transfer mechanisms. These transfer mechanisms ensure appropriate protection for individuals' rights and freedoms in respect of their personal data when it is transferred across borders. Alternative transfer mechanisms typically take the form of a binding and enforceable contract.

Article 46 of the UK GDPR provides for the following alternative transfer mechanisms:

- A legally binding and enforceable instrument between public authorities
- UK binding corporate rules
- Standard data protection clauses
- An approved code of conduct together with binding and enforceable commitments of the controller and processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights

- Certification under an approved certification scheme together with binding and enforceable commitments of the controller and processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights
- Bespoke contractual clauses authorised by the Information Commissioner
- Administrative arrangements between public authorities authorised by the ICO

In order to use an alternative transfer mechanism, the UK GDPR requires that the sender must be satisfied that the personal data will be appropriately protected. In practice, the process for organisations using the alternative transfer mechanisms to make an international transfer involves:

- Understanding what data is being transferred, to whom, and to where
- Identifying an appropriate transfer mechanism
- Undertaking a risk assessment to ensure that the alternative transfer mechanism provides the necessary protections and that there are enforceable data subject rights and effective redress, accounting for the laws and practices in the recipient country and any supplementary measures which may be required

256. Many organisations send data all over the world and often have a complex infrastructure to support such data sharing, including with organisations in countries that have not been assessed for adequacy, or with groups of organisations that operate across multiple jurisdictions. In order to make these transfers, organisations may rely on the alternative transfer mechanisms which incorporate the appropriate safeguards.

257. **The government intends to explore legislative change to ensure that the suite of alternative transfer mechanisms available to UK organisations in the UK GDPR is clear, flexible and provides the necessary protections for personal data.** Its ambition is to develop the regime for international transfer mechanisms in three broad ways:

    a. Proportionality: the safeguards applied during international transfers should be based on clear principles and proportionate to the risks facing data subjects in practice. When making an international data transfer, organisations must currently carry out case-by-case assessments to ensure that the alternative transfer mechanism provides the necessary protections and that there are enforceable data subject rights and effective redress, accounting for laws and practices in the recipient country and any supplementary measures which may be required. There is large variation between different countries' data protection regimes. Addressing risk can be challenging and time-consuming for organisations. Deciding what safeguards are necessary to transfer data without a significant degree of technical expertise can create large burdens for the small organisations without a significant degree of technical expertise.

    The government intends to clarify the legislation in order to facilitate more detailed, practical support for organisations on determining and addressing risks. This will help to create a more proportionate regime that both appropriately protects personal data and supports organisations to use alternative mechanisms with more confidence and ease.

b. Flexibility and future-proofing: the international data protection landscape and the ways that organisations use data will continue to change rapidly. Article 46 (2) of the UK GDPR includes a set of alternative transfer mechanisms that is exhaustive and constrained in form, and may not be sufficiently adaptable for the purposes of UK organisations and their international partners in the future. The limitations of a fixed set of transfer options become evident when considering possible future developments in the data protection landscape or particularly complex interdependent relationships, such as international networks of collaborating researchers.

   The government intends to explore amendments to the international transfers regime to give organisations greater flexibility in their use of transfer mechanisms. These changes will complement the work already underway by the ICO to support organisations to take greater advantage of the existing options for tailored transfer mechanisms, like Binding Corporate Rules, Codes of Conduct and Certification Schemes.

c. Interoperability: the UK's international transfer regime should have a flexible design which allows it to adapt, not only to businesses' specific transfer activities but also to mechanisms for international transfers developed by other countries or groups. New transfer mechanisms and new data protection practices are likely to develop as more countries and multilateral fora develop international transfer regimes. A regime that improves interoperability with such regimes will provide an advantage to UK businesses and consumers.

   The government wants the UK regime to have the capacity to be compatible with any potential new international transfer regimes regardless of the mechanisms they use to transfer data, as long as they can provide the necessary protections for data subjects.

258. Proposals to support the government's ambition to create a proportionate, flexible and more interoperable regime for alternative transfer mechanisms that provide the necessary protections are set out below.

Proportionality of appropriate safeguards

259. **To help organisations to determine the most appropriate safeguards for a particular personal data transfer, the government proposes to reinforce the importance of proportionality when using alternative transfer mechanisms.** Organisations and data subjects will benefit from greater clarity about how to make proportionate, outcomes-based decisions on what safeguards are reasonable. Further, these changes will ensure that the necessary safeguards are commensurate with the risks the transfers present and the likelihood of those risks occurring. Any legislative changes will be supported by the ICO through practical guidance on determining risks.

The government welcomes views on the following questions:

Q3.3.1. To what extent do you agree with the proposal to reinforce the importance of proportionality when assessing risks for alternative transfer mechanisms?

- *Strongly agree*
- *Somewhat agree*

- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q3.3.2. What support or guidance would help organisations assess and mitigate the risks in relation to international transfers of personal data under alternative transfer mechanisms, and how might that support be most appropriately provided?

Reverse transfers exemption

260. **The government proposes to exempt 'reverse transfers' from the scope of the UK international transfer regime.** After personal data originating overseas is transferred to the UK it falls under the scope of the UK GDPR.[81] Consequently a UK GDPR transfer mechanism must be used to make 'reverse transfers' back to the sender. This creates friction for UK businesses, without any clear benefit to data protection standards. This reform would make transfers that have been received by an organisation in the UK and are being sent back to the original transferor exempt from the international transfer regime. This is a proportionate change to remove unnecessary burdens where data is already subject to sufficient protection.

The government welcomes views on the following question:

Q3.3.3. To what extent do you agree that the proposal to exempt 'reverse transfers' from the scope of the UK international transfer regime would reduce unnecessary burdens on organisations, without undermining data protection standards?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Adaptable transfer mechanisms

261. **The government is considering whether to empower organisations to create or identify their own alternative transfer mechanisms in addition to those listed in Article 46 of the UK GDPR.** Such a change would benefit organisations with complex data transfer requirements, which could, for example, design and use bespoke contracts to enable safe international transfers. This would supplement the existing options for transfers in Article 46 of the UK GDPR

[81] This assumes that the personal data is not already under scope due to the extraterritorial provisions of UK GDPR.

and it would supersede the option currently in Article 46(3)(a) which provides for the development of bespoke data protection clauses, requiring proactive approval from the ICO.

262. Organisations that chose to create their own transfer mechanism would determine how the mechanism meets the requirements for appropriate safeguards. Organisations would be able to implement safeguards for international data transfers using the most appropriate means for their situation, for example, via the use of a novel mechanism like a bespoke contract without ICO approval. Such a reform might also permit transfers on the basis of protections provided for in another country's legislation.

263. What matters most is whether a transfer mechanism provides the appropriate levels of protection for individuals. Organisations that take advantage of the ability to create or identify their own international transfer mechanisms would still need to fulfil transparency and accountability requirements by, for example, undertaking impact assessments or clearly documenting the rationale to demonstrate that they have reasonable grounds for believing that the appropriate and enforceable safeguards are in place. Organisations will be supported via guidance from the ICO.

264. The proposed approach to empower organisations to choose or create their own transfer mechanism is similar to provisions in New Zealand's data protection regime under Information Privacy Principle 12. This principle permits organisations to transfer personal data overseas on the grounds that a foreign entity is required to protect the transferred personal information in a way that is comparable to the New Zealand Privacy Act (2020), including by relying on a binding contract, or by making an assessment of the laws in the recipient's jurisdiction. This principle fits alongside a range of other legal bases for international transfers, much like a comparable UK provision would sit alongside adequacy regulations, the transfer mechanisms in Article 46, and the derogations in Article 49 of the UK GDPR.

Explanatory box: *New Zealand Privacy Act 2020: Information Privacy Principle 12 on disclosure of personal information outside New Zealand*

On 1 December 2020, New Zealand's new Privacy Act came into force. It promotes early intervention and risk management, and enhances the role of the Privacy Commissioner. Changes also include strengthened protections for personal data when transferred overseas.

The Privacy Act requires that any cross-border disclosure of personal information is subject to laws that are equivalent to the privacy laws of New Zealand. International data transfers can be made:

- via a contractual obligation that provides a reasonable basis to believe that comparable safeguards will be upheld
- or via an assessment of the privacy laws in the recipient's jurisdiction

These provisions follow a principle of requiring a reasonable basis to believe that comparable safeguards will be upheld. The legislation does not prescribe the form of those contractual obligations or assessments. The New Zealand Office of the Privacy Commissioner has developed guidance to help organisations to comply with these rules and has published indicative model clauses.

The government welcomes views on the following questions:

Q3.3.4. To what extent do you agree that empowering organisations to create or identify their own alternative transfer mechanisms that provide appropriate safeguards will address unnecessary limitations of the current set of alternative transfer mechanisms?

- *Strongly agree*
- Somewhat agree
- Neither agree nor disagree
- Somewhat disagree
- Strongly disagree

Please explain your answer, and provide supporting evidence where possible.

Q3.3.5 What guidance or other support should be made available in order to secure sufficient confidence in organisations' decisions about whether an alternative transfer mechanism, or other legal protections not explicitly provided for in UK legislation, provide appropriate safeguards?

Q3.3.6. Should organisations be permitted to make international transfers that rely on protections provided for in another country's legislation, subject to an assessment that such protections offer appropriate safeguards?

- *Yes*
- *No*
- *Don't know*

Please explain your answer, and provide supporting evidence where possible.

A power to create new alternative transfer mechanisms

265. **The government proposes creating a new power for the Secretary of State to formally recognise new alternative transfer mechanisms.** This proposal would allow the Secretary of State to create new UK mechanisms for transferring data overseas or recognise in UK law other international data transfer mechanisms, if they achieve the outcomes required by UK law. This reform will help to future-proof the UK's approach to international transfers by allowing the UK to respond rapidly to international developments. For example, if other countries, or groups of countries, begin using new mechanisms to transfer data, the government will have the necessary powers to react quickly. Enabling UK organisations to use new mechanisms will ultimately mean the UK benefits from a more expansive set of transfer mechanisms that can operate across different regimes.

The government welcomes views on the following questions:

Q3.3.7. To what extent do you agree that the proposal to create a new power for the Secretary of State to formally recognise new alternative transfer mechanisms would increase the flexibility of the UK's regime?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q3.3.8. Are there any mechanisms that could be supported that would benefit UK organisations if they were recognised by the Secretary of State?

- *Yes*
- *No*
- *Don't know*

Please explain your answer, and provide supporting evidence where possible.

3.4 Certification Schemes

Explanatory box: *What are certification schemes?*

Certification schemes are voluntary, market-driven frameworks of context-specific rules that, under the UK GDPR, can be used to demonstrate a high standard of compliance and to provide appropriate safeguards for international transfers.

Certifications are characteristically framed at the sectoral or industry level, defining data protection rules and practices covering specific products, processes and services within the context of that sector, industry or similar group. Private bodies can develop criteria for certification schemes to the standards set in legislation and by the ICO. The criteria is submitted for assessment and prospective certification bodies are accredited by the UK Accreditation Service.

Once accredited, the certification body will assess prospective businesses to see if they meet the requirements to join the scheme. Certification schemes are complex measures that require significant time and resources to design, implement and maintain, and they demonstrate accountability and represent the highest standards of data protection.

266. **The government is considering modifications to the framework for certification schemes to provide for a more globally interoperable market-driven system that better supports the use of certifications as an alternative transfer mechanism.** The UK GDPR's accountability principle is central to certification. It is the requirement for organisations to take responsibility for what they do with personal data and how they comply with the UK GDPR.[82] Other jurisdictions take different approaches to defining how standards of accountability should be demonstrated. Their approaches can also require high standards of data protection, but present those

[82] See chapter 1 for more detail on accountability

requirements in different ways. However, if the accountability requirements for other countries are not compatible with the UK's then they will not be interoperable with the UK certifications system, precluding their use.

267. **To facilitate compatibility with a wider range of personal data protection regimes, the government proposes to allow certification to be provided for by different approaches to accountability.** The proposal would increase the potential of using certifications as a transfer mechanism by allowing more flexibility on how organisations demonstrate their accountability standards. For example these could be based on privacy management programmes. Privacy management programmes are risk-based organisational commitments, frameworks and controls that ensure a high standard of data protection as a matter of corporate responsibility. Section 2.2 in Chapter 2 provides more detail on privacy management programmes. The government will ensure the approach on accountability remains coherent across its use domestically and internationally. That approach is fundamental to the accountability frameworks of Singapore, Canada and Australia, for example.

268. **To bolster their use internationally, the government is considering provisions that clarify that prospective certification bodies outside of the UK can be accredited to run UK-approved international transfer schemes.** The government would encourage existing international schemes to engage with UK standards and bodies in other countries to develop UK-compliant schemes to support friction-free data flows with UK businesses.

The government welcomes views on the following questions:

Q3.4.1. To what extent do you agree with the approach the government is considering to allow certifications to be provided by different approaches to accountability, including privacy management programmes?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q3.4.2. To what extent do you agree that allowing accreditation for non-UK bodies will provide advantages to UK-based organisations?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q3.4.3. Do you see allowing accreditation for non-UK bodies as being potentially beneficial for you or your organisation?

- *Strongly agree*

- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain the advantages and risks that you foresee for allowing accreditation of non-UK bodies.

Q3.4.4. Are there any other changes to certifications that would improve them as an international transfer tool?

3.5 Derogations

Explanatory box: *What are derogations?*

The derogations described in Article 49 of the UK GDPR are exceptions from the general rule that you should not make a restricted personal data transfer unless it is covered either by a UK adequacy regulation, or there are appropriate safeguards in place. The use of derogations is the final mechanism available to organisations for transferring data internationally. Derogations can only be used in very limited circumstances and under specific conditions, where adequacy and alternative transfer mechanisms are unavailable.

Before considering derogations, organisations must first identify whether or not the recipient country is adequate, or whether appropriate safeguards can be used. If these mechanisms are not available, then the derogations can be considered. The available derogations are for situations where:

- the data subject 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 data subject and the controller, or pre-contractual measures taken at the data subject's request
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject 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 data subject or of other persons, where the data subject is physically or legally incapable of giving consent

- 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

If none of the derogations apply, organisations can consider one final option, referred to as 'compelling legitimate interest'. The use of this derogation is even more severely constrained than the other options. It can only be employed in circumstances where the transfer is not repetitive, the data only relates to a limited number of individuals and the transfer must be necessary for an organisation's compelling legitimate interest. To assess whether it can be used, organisations must balance their compelling legitimate interests against the impact on the rights and freedoms of the individuals the data relates to. Suitable additional safeguards like strict confidentiality agreements or additional technical controls should be used wherever possible. The details of how this transfer has been carried out must be recorded and both the data subjects and the ICO must be informed of the transfer.

269. The government proposes to maintain the existing overarching approach to derogations: they should be used only in situations where they are necessary and where neither adequacy nor other safeguards are appropriate. However, despite the strict conditions, there are still situations where derogations may be appropriate and a technical change may clarify the restrictions on using derogations.

Repetitive use of derogations

270. **The government proposes establishing a proportionate increase in flexibility for use of derogations by making explicit that repetitive use of derogations is permitted.** Repetitive use of derogations is currently restricted by the UK GDPR recitals and in European Union regulatory guidance.[83] This permission will apply to all of the derogations except the derogation for compelling legitimate interests. Making explicit that repetitive use of derogations is permitted will provide flexibility and assurance for organisations that need to rely on them in certain limited but necessary situations.

The government welcomes views on the following question:

Q3.5.1. To what extent do you agree that the proposal described in paragraph 270 represents a proportionate increase in flexibility that will benefit UK organisations without unduly undermining data protection standards?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

[83] Article 49 (1) (b) and (c)

3.6 Further Questions

Q3.6.1. The proposals in this chapter build on the responses to the National Data Strategy consultation. The government is considering all reform options in the round and will carefully evaluate responses to this consultation. ***The government would welcome any additional general comments from respondents about changes the UK could make to improve its international data transfer regime for data subjects and organisations.***

Q3.6.2. In your view, which, if any, of the proposals in 'Boosting Trade and Reducing Barriers to Data Flows' would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

Q3.6.3. In addition to any of the reforms already proposed in 'Boosting Trade and Reducing Barriers to Data Flows' (or elsewhere in the consultation), what reforms do you think would be helpful to make the UK's international transfer regime more user-friendly, effective or safer?

Chapter 4 - Delivering better public services

4.1 Introduction

271. The UK's experience of fighting the COVID-19 pandemic has demonstrated the power of using personal data responsibly in the public interest, and the benefits of collaboration between the public and private sectors. There is an opportunity to build on this experience in order to deliver public services in more agile, innovative, effective and efficient ways. Recent lessons about the operation and benefits of joined-up data use may also help to inform approaches to other governmental priorities, such as improving outcomes in education, the levelling-up agenda or the Net Zero target in relation to greenhouse gas emissions.

272. The challenges of collecting, using and sharing personal data to deliver better public services are well known. There are a number of barriers to effective data use in government, including: data infrastructure that is not interoperable; legal and cultural barriers to data sharing; inconsistent data capability in the workforce; and financial disincentives that discourage investment. The government also recognises that maintaining public trust is essential if more personal data is to be used for the purpose of improving the delivery of public services. Much of the personal data processed by government departments and other public authorities is sensitive in nature and the public rightly expects it to be processed fairly, transparently and securely.

273. The government is committed to building a truly joined-up and interoperable data ecosystem for the public sector that will address the limitations outlined above, whilst ensuring high levels of public trust. Effective leadership and coordination within government is key to addressing logistical and cultural barriers to data sharing. The newly established Central Digital and Data Office (CDDO) within the Cabinet Office will lead the next phase of digital transformation across the public sector. Its responsibilities will include: offering expert advice and counsel to Ministers and senior civil servants on the development and execution of digital, data, and technology strategies and policies; improving the interoperability of government data and standardisation of data sharing practices through the work of the Data Standards Authority; promoting and expanding the use of data sharing provisions in the Digital Economy Act 2017, and; maintaining and promoting the uptake of the Data Ethics Framework. Having the right data infrastructure, legislation, and ethical and trust frameworks are important foundations. Equally critical are governance, leadership and capability and these will also be a areas of focus of the CDDO, so that the capacity and skills are built to tackle the issues of today and the future.

274. The government's Technology Innovation Strategy, published in June 2019, noted that the public sector provides unique services and that the public's expectations are rising when it comes to digital public services. In 2020, the Centre for Data Ethics and Innovation (CDEI) conducted a survey of public attitudes towards data sharing which found that a majority of those surveyed (57%) understand why the government needs to use personal data to deliver services, compared to only 15% who do not. Research shows that the public is much more likely to view data sharing as acceptable if there is a public benefit.[84,85]

275. The rest of this chapter outlines a number of proposals to improve the delivery of government services through better use and sharing of personal data.

[84] Understanding Patient Data, 'Data for public benefit: the risks and benefits of data sharing'
[85] CDEI, 'Polling data: Data sharing between government departments' May 2021

4.2 Digital Economy Act 2017

276. Part 5 of the Digital Economy Act 2017 contains a single, umbrella piece of legislation that is designed to reduce legal barriers to data sharing and enable public authorities to share personal data for specific purposes. For public service delivery, this allows data sharing to support services and positive interventions for individuals and households as part of social and economic policies. The Digital Economy Act 2017 can be used where there are no existing statutory gateways and where consent cannot be relied on or is not appropriate.

277. The Cabinet Office is committed to driving forward the use of powers in the Digital Economy Act 2017 across government, as well as addressing barriers to data sharing more widely. To facilitate more responsive, joined-up public services, work is underway to explore how to extend the public service delivery powers under section 35 of the Digital Economy Act 2017 to business undertakings. Businesses can benefit from public services across our digital economy - for example, by using digital verification services, or accessing support when trying to start up new businesses, or applying for government grants like the Bounce Back Loans. This would build on the powers that are already in place to support individuals and households with multiple disadvantages and alleviate fuel and water poverty.

The government welcomes views on the following question:

Q4.2.1. To what extent do you agree with the following statement: 'Public service delivery powers under section 35 of the Digital Economy Act 2017 should be extended to help improve outcomes for businesses as well as for individuals and households'?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

4.3 Use of Personal Data in the COVID-19 Pandemic

278. The COVID-19 pandemic has resulted in many different organisations in the public, private and voluntary sectors processing personal data concerning health in novel and responsible ways in order to combat the COVID-19 virus. Domestically, for example, government departments have worked closely with supermarkets to make delivery slots available for vulnerable people. Restaurants, pubs and other venues have collected visitors' logs and shared that data with health authorities in the event of a confirmed infection at their establishments. Airports have introduced screening procedures to help keep passengers safe. Internationally, labs at the forefront of tackling the outbreak have shared information to help researchers develop tests for the COVID-19 virus.

279. Despite the challenges and novel situations presented by the COVID-19 pandemic, it usually has been possible for organisations to find a way to process personal data lawfully whenever it is necessary for public health purposes. There have been instances, however, in which a lack of

clarity in the law meant that data controllers and policy-makers had to spend a considerable amount of time and resources making sure new processing activities were compliant.

Private companies processing personal data to help deliver public tasks

280. To process personal data in order to deliver public tasks that are set out in law, public authorities will usually rely on Article 6(1)(e) of the UK GDPR as the lawful basis of processing. The situation can be less clear for private bodies that are processing data at the request of public authorities in order to help deliver public tasks. The private sector has played a crucial role in helping healthcare providers tackle the COVID-19 virus - for example, mobile phone companies have been asked to send important public health messages to different groups, and digital platforms have contributed to the development of contact tracing applications. Private companies have generally been able to identify a relevant lawful ground for undertaking such processing. Depending on the circumstances, some have been processing health data in compliance with legal obligations under Article 6(1)(c) of the UK GDPR; others have relied on the legitimate interest ground under Article 6(1)(f) of the UK GDPR.

281. Reliance on Article 6(1)(f) has been complicated at times because it has required the data controller to undertake an assessment of whether its own interests outweigh the data protection rights of individuals, when often the wider public benefits of the processing activity constitute the main interest at issue. The onus should not be on individual data controllers in the private sector to undertake legitimate interests assessments when they have been asked to undertake the processing by government departments in order to assist the delivery of public tasks.

282. **The government therefore proposes to clarify that private companies, organisations and individuals who have been asked to process personal data on behalf of a public body may rely on that body's lawful ground for processing the data under Article 6(1)(e) of the UK GDPR and need not identify a separate lawful ground.** Processing by private bodies for such purposes may need to be subject to certain safeguards. For example, a public body may be required to clarify its powers or basis in law for directing the processing activity in the first place; and the private bodies carrying out the processing activity would not be allowed to continue to rely on Article 6(1)(e) once the relevant public task was complete or reuse the data for other purposes. To retain public trust in processing by private sector organisations on behalf of public authorities, it may also be important to ensure that there is no reduction in people's ability to exercise their rights in relation to any personal data being processed, including in respect of exercising the rights to object. This proposal would not affect the operation of Article 6(1)(e) more broadly and it would remain the main lawful ground for public authorities processing personal data in connection with public tasks set out in law.

283. This change would also support effective collaboration between the public and private sector in any future public health emergency, or in relation to other matters of public interest. For example, if a private company were asked to share information with law enforcement or intelligence agencies for the purposes of preventing crime, it could point to the relevant agency's lawful ground for processing the data. It would not, however, compel disclosure and the controller would remain free to determine whether or not to make the disclosure. This would complement the changes proposed in Chapter 1 to the legal ground of legitimate interests for processing. The government envisages that a data controller wishing to make an unplanned or reactive disclosure to the police - for example, to report a crime - could rely on the lawful ground of legitimate interests. Meanwhile, a data controller that is regularly sharing information with the law enforcement agencies at their request could rely on those bodies' lawful grounds for processing the data under Article 6(1)(e).

The government welcomes views on the following questions:

Q4.3.1. To what extent do you agree with the following statement: 'Private companies, organisations and individuals who have been asked to process personal data on behalf of a public body should be permitted to rely on that body's lawful ground for processing the data under Article 6(1)(e) of the UK GDPR'?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, providing supporting evidence where possible.

Q4.3.2. What, if any, additional safeguards should be considered if this proposal were pursued?

Processing health data in an emergency

284. As well as identifying a lawful ground under Article 6 of the UK GDPR, any data controller which is processing health data must also identify a ground under Article 9 of the UK GDPR. This is because health data is classed as sensitive personal data and is subject to heightened safeguards. Under the current law, data regarding a person's health can generally only be processed where: the individual has given explicit consent; it is necessary for health, social care or public health purposes overseen by healthcare professionals; it is necessary for other specified purposes, such as scientific research; or it is necessary for other reasons of substantial public interest, as defined in Schedule 1 to the Data Protection Act 2018.

285. During the COVID-19 pandemic, it has occasionally been complex to identify a relevant ground under Article 9 for the relevant processing activity. This is because the legal ground for processing data for public health purposes currently requires the oversight of a healthcare professional or for the processing to be carried out by a data controller acting under a duty of confidentiality.[86] In situations when non-healthcare bodies have been required to process personal data, it has not always been obvious how to meet these criteria. Pragmatic and helpful guidance issued by the ICO has generally helped to remove uncertainty but there is a case for using legislation to rectify this ambiguity.

286. **To address this issue, the government proposes to clarify that public and private bodies may lawfully process health data when necessary for reasons of substantial public interest in relation to public health or other emergencies.** This permission is irrespective of whether the processing is overseen by healthcare professionals or undertaken under a duty of confidentiality. Such processing would still need to be time-limited and subject to appropriate safeguards that reflect the sensitivity of the data. This measure may help to reassure data controllers that the data protection framework will not pose unreasonable barriers when they are designing processing activities which support the government's response to an emergency.

[86] Schedule 1 to the Data Protection Act 2018, para 3

The government welcomes views on the following questions:

Q4.3.3. To what extent do you agree with the proposal to clarify that public and private bodies may lawfully process health data when necessary for reasons of substantial public interest in relation to public health or other emergencies?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, providing supporting evidence where possible.

Q4.3.4. What, if any, additional safeguards should be considered if this proposal were pursued?

4.4 Building Trust and Transparency

287. Public trust is vital to the delivery of better public services and outcomes for individuals. This section outlines measures to strengthen the transparency and clarity of personal data processing by the public sector. Public bodies should also be empowered to share and utilise more personal data in the public interest, while safeguarding data subjects' rights and interests.

Transparency mechanisms for algorithms

288. There are clear benefits to organisations, individuals and society in explaining algorithmic decision-making in the public sector. Providing explanations to individuals affected by such a decision can help organisations, including in the public sector, ensure greater fairness in the outcomes for different groups across society.

289. The UK's current data protection framework already recognises the importance of public trust by imposing specific requirements on public authorities.

290. **The government proposes introducing compulsory transparency reporting on the use of algorithms in decision-making for public authorities, government departments and government contractors using public data**. This would provide much greater information about, for example, what datasets are being used, technical specifications of the algorithms, and how ethical considerations, such as mitigating bias, are addressed.

The government welcomes views on the following questions:

Q4.4.1. To what extent do you agree that compulsory transparency reporting on the use of algorithms in decision-making for public authorities, government departments and government contractors using public data will improve public trust in government use of data?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your choice, and provide supporting evidence where possible.

Q4.4.2. Please share your views on the key contents of mandatory transparency reporting.

Q4.4.3. In what, if any, circumstances should exemptions apply to the compulsory transparency reporting requirement on the use of algorithms in decision-making for public authorities, government departments and government contractors using public data?

Processing in the 'substantial public interest'

291. Sensitive personal data ('special category data' under Article 9 of the UK GDPR, and criminal convictions and offences data under Article 10 of the UK GDPR) includes, for example, personal data relating to a person's health, racial or ethnic origins, political opinions or sexual orientation. It can also include genetic data and biometric data such as fingerprints, DNA or facial images.[87] The default position is that sensitive data cannot be processed unless there is explicit consent from the data subject, or it is expressly permitted for purposes listed in the UK GDPR and Schedule 1 to the Data Protection Act 2018.

292. The UK GDPR and Schedule 1 to the Data Protection Act 2018 set out a range of situations when such sensitive data may be processed, and various tests or conditions that must also be met. These range from situations requiring sensitive data processing needed for counselling purposes, MPs' constituency casework or to promote diversity at senior levels in organisations.

293. There are two key challenges to consider. The first is finding the balance between ensuring provisions are sufficiently flexible to allow all necessary processing of sensitive data, and ensuring provisions are specific enough to give data subjects transparency and controllers certainty. **The government is considering whether to add new situations to those in Schedule 1, or to amend existing situations in order to provide greater specificity.**

294. The second key challenge is ensuring that each provision has the right safeguards or limitations in order to avoid misuse, and to provide greater transparency and certainty to data subjects and controllers. Part 2 of Schedule 1 to the Data Protection Act 2018 sets out situations where certain categories of sensitive data can be processed for reasons of 'substantial public interest', as per Article 9(2)(g) UK GDPR. In certain situations the controller must apply a test of whether the processing would be in the 'substantial public interest'. This test is not required in other situations or for purposes that are deemed to always be in the 'substantial public interest' - for example, processing for the administration of justice.

295. The government has heard from some stakeholders that these rules are not sufficiently defined and there is no case law to assist with its interpretation. Data controllers may struggle to differentiate between 'public interest' and 'substantial public interest', given potential uncertainty about both terms. This uncertainty may discourage or delay data controllers from processing or

[87] CIO Guidance: Special category data

sharing sensitive data, even when there is a strong or urgent case in the public interest for doing so.

296. **One option to tackle this uncertainty is to include in legislation a definition of 'substantial public interest'**. Such a definition could provide reassurance or at least greater certainty to organisations that are hesitating over whether their purposes for processing constitute a substantial public interest. A key challenge would be to ensure the definition is not so narrow and rigid that it precludes lesser known or future purposes that ought to meet the test, and that it is not so broad and open to allow processing that could not have reasonably been expected.

297. **Another option is to add to or amend the list of specific situations in Schedule 1 to the Data Protection Act 2018 that are deemed to always be in the substantial public interest.** These would need to be considered carefully so that a high level of protection for individuals is maintained, but could include, for example, processing that is necessary for the purposes of safeguarding national security.

The government welcomes views on the following questions:

Q4.4.4. To what extent do you agree there are any situations involving the processing of sensitive data that are not adequately covered by the current list of activities in Schedule 1 to the Data Protection Act 2018?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer and provide supporting evidence where possible, including on:

- *What, if any, situations are not adequately covered by existing provisions*
- *What, if any, further safeguards or limitations may be needed for any new situations*

Q4.4.5. To what extent do you agree with the following statement: 'It may be difficult to distinguish processing that is in the substantial public interest from processing in the public interest'?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q4.4.6. To what extent do you agree that it may be helpful to create a definition of the term 'substantial public interest'?

- *Strongly agree*
- *Somewhat agree*

- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible, including on:

- *What the risks and benefits of a definition would be*
- *What such a definition might look like*
- *What, if any, safeguards may be needed*

Q4.4.7. To what extent do you agree that there may be a need to add to, or amend, the list of specific situations in Schedule 1 to the Data Protection Act 2018 that are deemed to always be in the substantial public interest?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible, including on:

- *What such situations may be*
- *What the risks and benefits of listing those situations would be*
- *What, if any, safeguards may be needed*

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

298. The legal framework should provide clarity and transparency on the processing of personal data by the public sector. It must also provide the UK's law enforcement and national security communities with the tools to adapt to changing circumstances across all sectors and respond rapidly to emerging threats.

299. Biometric technologies like DNA analysis, fingerprints and, increasingly, facial image recognition are important tools in tackling knife crime, child sexual exploitation, terrorism and other offences. The public rightly expects the police to use biometrics appropriately to protect public safety within a framework that is fair, transparent and proportionate.

300. There is already a comprehensive legal framework in place covering use of biometric data for law enforcement purposes, but it is complex for both the police and the public to understand. This is a fast-developing area, with technological advancements regarding biometrics data, and the legal framework needs to be capable of keeping pace. Unless addressed, this could inhibit the confident adoption of new technologies that can improve public safety.

301. **The government is therefore considering changes to make the legislative framework simpler, more transparent and flexible by streamlining and clarifying rules on the collection, use and retention of data for biometrics by the police.**

302. We intend to build on the current detailed rules that apply to the collection, use and retention of biometric data by the police, including the possibility of issuing additional codes of practice under Part 3 of the Data Protection Act 2018. The use of codes of practice to provide guidance could help to explain the application of data protection laws and provide valuable support to law enforcement. By pursuing our ambition to align more closely the commercial, law enforcement and national security processing frameworks, it is important to have the flexibility to bring both further clarity to the police and greater transparency to the public.

The government welcomes views on the following question:

Q4.4.8. To what extent do you agree with the following statement: 'There is an opportunity to streamline and clarify rules on police collection, use and retention of data for biometrics in order to improve transparency and public safety'?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, providing supporting evidence where possible.

4.5 Public Safety and National Security

303. The preceding proposals seek to clarify the circumstances in which data can be processed and provide controllers with greater confidence to process and use data in the public interest. It is also vital that this reform agenda can enhance the work of our law enforcement bodies and UK Intelligence Services in the interests of public safety.

304. To encourage and facilitate the effective sharing of data for law enforcement and national security purposes, we consider there is value in seeking to minimise differences and improve consistency across the commercial, law enforcement and national security processing regimes. Greater consistency between the regimes and additional clarity on data sharing between controllers operating under different rules will ensure that both the public and controllers have a better understanding of how and when data is used to maximise the opportunities to support cross-sector working.

305. To drive consistency across the UK GDPR, Part 3 (Law Enforcement processing) and Part 4 (Intelligence services processing) of the Data Protection Act 2018, the government intends to explore whether it is possible to align key terms that are used across these different data processing frameworks. Differences between each of these processing frameworks is to be expected, given they were drafted to apply to specific types of processing. Nonetheless the standardisation of terminology and definitions, where appropriate, could provide controllers with greater clarity on their obligations and confidence to the public on how data is being used.

306. **To build on the wider reform proposals that support better private and public sector collaboration, the government will seek to clarify the legislation to facilitate improved cross-sector working, which will support in particular the joint operational activity between law enforcement and national security partners.** For example, currently controllers

processing personal data under Part 3 or Part 4 of the Data Protection Act 2018 can only be regarded as joint controllers with other controllers processing under the same part of the Act. The government intends to amend the provisions for joint controllership to enable controllers operating under Part 3 and Part 4 of the Data Protection Act 2018 to collaborate better.

The government welcomes views on the following question:

Q4.5.1. To what extent do you agree with the proposal to standardise the terminology and definitions used across UK GDPR, Part 3 (Law Enforcement processing) and Part 4 (Intelligence Services processing) of the Data Protection Act 2018?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

4.6 Further Questions

Q4.6.1. In your view, which, if any, of the proposals in 'Delivering Better Public Services' would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

Q4.6.2. In addition to any of the reforms already proposed in 'Delivering Better Public Services' (or elsewhere in the consultation), what reforms to the data protection regime would you propose to help the delivery of better public services?

Chapter 5 - Reform of the Information Commissioner's Office

5.1 Introduction

307. The Information Commissioner's Office (ICO) is the independent supervisory authority with responsibility for monitoring and enforcing the application of data protection legislation in the UK. The Information Commissioner is accountable to Parliament and may be called to give evidence to the DCMS Select Committee. DCMS is the sponsoring government department of the ICO and the Secretary of State for DCMS is responsible for the ICO in Parliament.

Explanatory box: *The ICO's regulatory mandate and functions*

The ICO has an important, complex and wide-ranging mandate. In addition to being responsible for the regulation of personal data protection, the ICO is tasked with the regulation of freedom of information and is empowered to take various regulatory actions under eleven pieces of legislation:

- The UK General Data Protection Regulation
- The Data Protection Act 2018
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information Act 2000
- The Environmental Information Regulations 2004
- The Environmental Protection Public Sector Information Regulations 2009
- The Investigatory Powers Act 2016
- The Re-use of Public Sector Information Regulations 2015
- The Enterprise Act 2002 (EnA 2002)
- Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)
- The Network and Information Systems Regulations 2018 (NIS Regulations)

In line with these responsibilities, the ICO has an array of important public-facing functions, including giving advice to members of the public about their information rights and obligations; responding to and, if necessary, investigating complaints lodged by members of the public; and taking action to enhance the information rights practices of organisations and enforcing the law.

Moreover, the ICO plays a crucial role in upholding and developing information rights practices internationally, and has a number of international obligations. The ICO's mandate is not sector-specific, adding breadth and complexity to its various functions and obligations.

308. As part of fulfilling its sponsorship role, DCMS works closely with the ICO in order to ensure high standards of data protection are implemented effectively in the UK. As part of its existing transformation programme, the ICO is working to increase its valuable, upstream support to help organisations comply with the law, and develop its consultative approach to guidance with a greater emphasis on how organisations may use and share data responsibly. For example, the

ICO's recent Data Sharing Code of Practice recognises the centrality of data sharing to driving digital innovation in both the private and public sectors, and offers practical advice to give organisations the confidence to share data in a fair, safe and transparent way.

309. Looking ahead, the government wants to empower the Information Commissioner to protect data rights and promote trust in the data protection system in order to unlock the power of data. A modernising reform agenda is an investment in the ICO's future success and will sustain its world-leading reputation, while preserving its regulatory independence. The recruitment of a new Information Commissioner this year will help to embed this agenda at the very top of the ICO.

310. The ICO must continue to be an agile and forward-looking regulator, investing in its horizon-scanning functions and intelligence gathering capabilities in order to keep pace with new technologies and emerging regulatory issues. The ICO should seek to intervene early to prevent irresponsible practices before they can cause widespread harm, and encourage innovation and responsible data use that drives growth.

311. The government's proposed reforms will better equip the ICO to play this regulatory role by creating a clearer mandate for a risk-based and proactive approach to its regulatory activities in line with best practice of other regulators. This should allow the ICO to, for example: increase its strategic outreach to sectors that are using personal data in new and innovative ways, including financial services, healthcare and marketing; enhance its sandbox function to provide greater opportunities for organisations to test new and innovative products in a safe way, and; provide greater support to small and medium-sized enterprises.

312. As set out in detail below, the government intends to improve the legislative framework that underpins the ICO by: setting new and improved objectives and a clearer strategic vision for the regulator; improving accountability mechanisms, and; refocusing its statutory commitments away from handling a high volume of low-level complaints and towards addressing the most serious threats to public trust and inappropriate barriers to responsible data use. In the future, the ICO should devote more resources to supporting those organisations that want to innovate responsibly and tackling poor practices by those that do not meet the UK's high standards for data protection.

313. The rise in uptake of digital technologies is challenging existing regulatory structures and governments around the world are taking steps to respond. The government will put in place mechanisms to ensure the ICO continues to work closely with other regulators in order to ensure a coherent, innovation-friendly and streamlined regulatory landscape, thereby achieving better regulatory outcomes in digital markets. This will be done in relation to the government's Plan for Digital Regulation which sets out three objectives for digital regulation:

    a. Actively promoting competition and innovation in the digital economy

    b. Keeping the UK safe and secure online

    c. Shaping a digital economy that promotes a flourishing, democratic society

314. The government's data reform agenda will be an important facet of the overall approach and will contribute to all three objectives, guided by principles that will create proportionate, agile and flexible measures. These principles include: actively promoting innovation; achieving forward-looking and coherent outcomes; and exploiting opportunities and addressing challenges in the international arena. This work will be consistent with the government's approach to other digital

regulation activities such as the new online safety framework and the pro-competition regime for digital markets.

315. In line with the Plan for Digital Regulation, the government wants to equip digital regulators with the right capabilities to respond quickly to the latest innovations in markets and digital technologies. The ICO should continue to collaborate effectively with other digital regulators as the fast-moving and cross-cutting nature of digital technologies means that regulatory regimes may become increasingly interconnected.

316. This approach is consistent with the proposals set out in the government's consultation on Reforming the Framework for Better Regulation in line with the move to smarter and more agile regulation. The consultation reviews the role of regulators, especially in relation to competition and innovation, and proposes more discretion for regulators to achieve their objectives in a flexible way, counterbalanced by increased accountability and scrutiny.

317. The ICO currently receives a small amount of Grant In Aid funding from the government for its statutory responsibilities in relation to the Freedom of Information Act, Network and Information Systems Regulations, Investigatory Powers Act and legislation in relation to electronic identification and trust services. Its statutory responsibilities in relation to data protection are funded by organisations that pay the data protection fee, which accounts for the majority of the ICO's funding overall. The government will continue to monitor the efficacy of the ICO's funding model and fee structure and, if necessary, consult on any changes in light of the reforms to the ICO set out below.

318. The reform proposals outlined in sections 5.2 (Strategy, Objectives and Duties), 5.5 (Codes and Guidance), 5.6 (Complaints), and 5.7 (Enforcement) relate to the ICO's remit for data protection only. The reform proposals outlined in sections 5.3 (Governance Model and Leadership), and 5.4 (Accountability and Transparency) relate to the ICO's entire remit.

319. The government is committed to the ICO's status as an independent regulator. This is particularly important for the ICO's role in the regulation of public bodies, both for data protection and freedom of information.

5.2 Strategy, Objectives and Duties

320. Currently, the UK GDPR does not provide the ICO with a clear framework of objectives and duties against which to prioritise its activities and resources, evaluate its performance and be held accountable by its stakeholders. Instead, the ICO is obliged to fulfil a long list of tasks, as set out in Article 57 of the UK GDPR, but without a strategic framework to guide its work. The ICO has started to fill this gap by publishing documents, such as its Information Rights Strategic Plan, which sets out strategic objectives and goals. This is complemented by documents on specific areas, such as its Technology Strategy and International Strategy. A clearer set of statutory strategic objectives for the ICO could offer greater clarity and stability to the ICO's role and purpose, improve transparency, and strengthen accountability in line with best practice of other regulators.

321. **The government proposes to introduce a new, statutory framework that sets out the strategic objectives and duties that the ICO must fulfil when exercising its functions.** As the ICO's role becomes increasingly important for competition, innovation and economic growth, this strategic framework should empower the ICO to take greater account of impacts in these other domains as it supervises and enforces the UK's data protection regime. As an independent

regulator, the ICO would continue to set its operational objectives in order to ensure it effectively delivers against this framework.

322. **In addition, the government proposes to introduce a power for the Secretary of State for DCMS to prepare a statement of strategic priorities** to inform how the ICO sets its own regulatory priorities. The introduction of this power will bring the ICO into line with regulators such as Ofcom, Ofwat and Ofgem. This proposal is set out in paragraphs 344-346.

323. These proposals relate to the ICO's remit for data protection only. The government has taken into account the ICO's regulatory oversight of the public sector when considering these proposals in order to ensure its independence is preserved.

Overarching objective

324. An overarching objective, which sits at the top of a hierarchy of objectives and duties, will ensure the ICO's primary role and priorities are clear. This hierarchy will be particularly important in the event of any conflict between its objectives and duties.

325. **The government proposes to introduce a new overarching objective for the ICO, in addition to its other functions, tasks and duties. We propose two elements to this objective:**

    a. Upholding data rights: this element of the overarching objective, based on existing legislation, would ensure the ICO can monitor the application of data protection legislation, uphold the data rights of individuals, and safeguard personal data from misuse.

    b. Encouraging trustworthy and responsible data use: this element of the objective would ensure the ICO will uphold the public's trust and confidence in use of personal data.

The government welcomes views on the following questions:

Q5.2.1.To what extent do you agree that the ICO would benefit from a new statutory framework for its objectives and duties?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q5.2.2. To what extent do you agree with the proposal to introduce an overarching objective for the ICO with two components that relate to upholding data rights and encouraging trustworthy and responsible date use respectively?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q5.2.3. Are there any alternative elements that you propose are included in the ICO's overarching objective?

- *Yes*
- *No*
- *Don't know*

Please explain your answer, and provide supporting evidence where possible.

Growth and innovation duty

326. The ICO, along with most national non-economic regulators in the UK, has a statutory duty under the Deregulation Act 2015 to take into account the desirability of promoting economic growth (the 'growth duty'), as well as an obligation under the Regulators' Code to support economic growth.[88,89] The growth duty requires a regulator to consider the importance of the promotion of economic growth whenever it exercises one of its regulatory functions. The Regulators' Code, as provided for under the Legislative and Regulatory Reform Act 2006, sets out a clear, flexible and principles-based framework for how regulators should engage with those they regulate.

327. Both the growth duty and the Regulators' Code offer a set of useful principles to guide a proportionate and risk-based approach to regulation. However, these principles are broad because they apply to all non-economic regulators, whose regulatory functions have varying impacts on economic growth. Crucially, accountability mechanisms for both leave considerable leeway for regulators to determine and report on compliance.

328. The ICO's remit is increasingly important for competition, innovation and economic growth, especially when compared with many other regulators to which the existing growth duty applies. The ICO recognises this and sets out in various documents how it discharges its functions with respect to the growth duty. The ICO's Regulatory Policy Methodology Framework, for example, references the growth duty and explains how the ICO needs to decide how to balance trade-offs between competing priorities when delivering on its responsibilities. As digital technologies and their applications drive innovation across every part of the UK economy, it is important for the ICO, as one of the key regulators in the digital economy, to continue to improve on and be accountable for its regulatory approach with respect to impacts on competition, innovation and economic growth.

329. **The government proposes to strengthen the ICO's existing obligations by placing a new duty on it to have regard for economic growth and innovation when discharging its functions.**

330. This new requirement would not conflict with the existing growth duty or the principles under the Regulators' Code, and would specify many of the same principles and guidelines in the context of the ICO's activities. Additionally, this new requirement aligns with the Plan for Digital Regulation's

[88] As specified in the Economic Growth (Regulatory Functions) Order 2017, UK Statutory Instruments, 2017 No. 267

[89] As specified in the Legislative and Regulatory Reform (Regulatory Functions) Order 2007, UK Statutory Instruments2007, No. 3544

core principle for regulators to actively promote innovation. Specific obligations under the new duty could include:

a. Providing evidence of how the development of regulatory policy takes account of economic growth and innovation, especially in emerging technologies - for example, by undertaking an in-depth market condition analysis via business surveys and regular engagement with regulated communities

b. Systematic analysis or 'horizon scanning' for threats and opportunities across sectors

c. Evaluations of interventions on market conditions, and publication of outcomes and lessons learnt

331. As part of the new obligations, the ICO would be required to set out in its regulatory approach how it intends to comply with the duty and report against how due regard to the duty was given when discharging its functions. Further information on proposed transparency requirements is set out in section 5.4.

The government welcomes views on the following question:

Q5.2.4. To what extent do you agree with the proposal to introduce a new duty for the ICO to have regard to economic growth and innovation when discharging its functions?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Competition duty

332. In May this year, the ICO and the Competition and Markets Authority (CMA) published a joint statement on competition and data protection in digital markets, which describes the interactions between the regulators and their respective regimes. This joint statement builds on the ongoing collaboration between the ICO, CMA, Ofcom and Financial Conduct Authority through the Digital Regulation Cooperation Forum (DRCF). The DRCF was set up by the CMA, the ICO and Ofcom in July 2020 to support regulatory coordination in online services and cooperation on areas of mutual importance.

333. This highlights how regulatory interventions to promote competition and data protection can be productively aligned and are often mutually reinforcing - for example, when enhancing user choice and control. Tensions may also exist between regulatory objectives, such as increasing access to personal data in pursuit of better competition outcomes. The ICO and CMA highlight that close cooperation will be vital to ensure that these tensions are managed well.

334. As demonstrated by the joint statement, the ICO and CMA are already working productively together. The government nonetheless wants to provide a stronger statutory underpinning to this

collaboration in order to reinforce cooperation across the digital regulatory landscape and, in this context, ensure more transparency on how the ICO considers competition issues.

335. **The government proposes to introduce a duty for the ICO to have regard to competition when discharging its functions.** This duty would not supersede its overarching objective, but ensure that the ICO is equipped to factor in interactions with competition when discharging its core functions.

336. Similarly to the growth and innovation duty, the ICO would be required to set out in its regulatory approach how it intends to comply with the duty and report against how due regard to the duty was given when discharging its functions. Further information on proposed transparency requirements is set out in section 5.4.

The government welcomes views on the following question:

Q5.2.5. To what extent do you agree with the proposal to introduce a duty for the ICO to have regard to competition when discharging its functions?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Collaboration and enhanced information sharing gateways

337. Addressing the interactions between data protection and competition regimes is just one of the regulatory challenges posed by digital innovation. New digital services or products, and disruptive business models are increasingly cutting across traditional regulatory boundaries. This means that it will become more important for digital regulators to take into account how their regulatory activities and interventions interact with one another and draw on their respective expertise where relevant.

338. **Building on evidence supplied by the Digital Regulation Cooperation Forum (DRCF), the government proposes to introduce a new duty on the ICO to cooperate and consult with other regulators, in particular those in the DRCF.**[90] There is precedent for this within the financial services regime, where consultation is required before certain types of decisions are implemented. For example, the Financial Services and Markets Act 2000 and 2013 establish duties on the Financial Conduct Authority, Bank of England, Prudential Regulation Authority and

[90] DRFC, 'Embedding coherence and cooperation in the fabric of digital regulators', the DRCF have proposed a number of measures to enhance regulatory coordination between the key digital regulators. These include new duties to consult, requiring regulators to consult with each other where they have relevant expertise to inform decision-making; new duties to cooperate, requiring regulators to put in place appropriate mechanisms to support cooperation; and the creation of statutory information sharing gateways that would facilitate joint work between regulators.

Public Sector Resourcing to coordinate their activities, embedding requirements to consult and cooperate.[91,92]

339. The government is also examining ways to improve information sharing between the ICO and other regulators in order to allow more effective and efficient cooperation, for example, by reducing duplicative information requests. **The government is therefore exploring whether to establish a new information sharing gateway to enable regulators, in particular those in the DRCF, to share information in support of cooperation across a broad range of issues.**[93] Any such information sharing gateways would, however, need to be carefully designed with appropriate safeguards.

The government welcomes views on the following questions:

Q5.2.6. To what extent do you agree with the proposal to introduce a new duty for the ICO to cooperate and consult with other regulators, particularly those in the DRCF (CMA, Ofcom and FCA)?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q5.2.7. Are there any additional or alternative regulators to those in the Digital Regulation Cooperation Forum (CMA, Ofcom and FCA) that the duty on the ICO to cooperate and consult should apply to?

- *Yes*
- *No*
- *Don't know*

Please explain your answer, and provide supporting evidence where possible.

Q5.2.8. To what extent do you agree with the establishment of a new information sharing gateway between relevant digital regulators, particularly those in the DRCF?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

[91] Financial Services and Markets Act 2000, s.3D-H

[92] Financial Services (Banking Reform) Act 2013, s.98-102,

[93] Information sharing gateways are legislative clauses which permit regulators to share confidential information with each other if it is deemed necessary for the delivery of particular functions set out in the gateway. The DRCF has proposed introducing a gateway which would enable digital regulators to share information to enable joint working. This would create a more reciprocal and continuous form of information sharing.

Q5.2.9. Are there any additional or alternative regulators to those in the DRCF (ICO, CMA, Ofcom and FCA) that the information sharing gateway should include?

- *Yes*
- *No*
- *Don't know*

Please explain your answer, and provide supporting evidence where possible.

Public safety duty

340. Data protection has practical implications for the vital work of the UK Intelligence Services and law enforcement bodies. It impacts processing undertaken in the interests of public safety, and on the public's trust in the use of their data. Data capabilities, developing technologies and their differing uses will also pose new challenges to the application of data protection policies.

341. The law already provides for bespoke regimes which are applicable when processing personal data for a law enforcement purpose (Part 3 of the DPA) or where processing is by or on behalf of the intelligence services (Part 4 of the DPA). This serves as a useful reminder of the special nature of this processing, which contributes to the protection of the rights and freedoms of the general public.

342. It will be increasingly important for the ICO to take into account how its regulatory activity interacts with the statutory functions of bodies that serve to protect the public, as well as draw on relevant expertise to enable data controllers to effectively use data, operate the legislation and build public trust.

343. **The government is proposing to provide clarity on this important element of the ICO's considerations by introducing specific language recognising the need for the ICO to have due regard to public safety when carrying out its functions.** The purpose of this proposal is not to introduce additional obligations on the ICO, but to reiterate an important factor that already exists when the ICO is responding to public safety challenges during the discharging of its core functions. This duty would not supersede the ICO's overarching objective.

The government would welcome views on the following question:

Q5.2.10. To what extent do you agree with the government's proposal to introduce specific language recognising the need for the ICO to have due regard to public safety when discharging its functions?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer and provide supporting evidence where possible.

Statement of strategic priorities

344. The importance of data to our economy and the broad, cross-sectoral scope of the ICO's remit mean that the ICO is one of the UK's most significant regulators. Its decisions on how personal data can be used may affect scientific research, innovation and delivery of public services and the performance of many parts of the UK's economy. The rapid technological changes arising from the use of personal data put an onus on operating a flexible and responsive regulatory framework that enables the ICO to proactively address the emerging challenges and the wider policy context in which it operates.

345. **The government proposes to introduce a new power for the Secretary of State for DCMS to periodically prepare a statement of strategic priorities to which the ICO must have regard when discharging its functions.** The purpose of the statement would be to enable the government to identify and convey those domestic and international priorities that form an important context in which the ICO sets its own regulatory priorities.

346. This proposal is comparable to the UK's wider regulatory regime; similar powers apply to other regulators such as Ofcom,[94] Ofgem,[95] and Ofwat.[96] As an independent regulator, the ICO will not be bound by the statement of strategic priorities. Instead, the ICO will be expected to respond to the statement, and explain whether and how its work addresses the priorities set out by the government. This is not intended to conflict with the ICO's statutory objectives, duties, functions and tasks, which would take precedence if any conflict were to arise. This is particularly important given the ICO's role in regulating the public sector and the importance of preserving its independence.

The government welcomes views on the following question:

Q5.2.11. To what extent do you agree with the proposal for the Secretary of State for DCMS to periodically prepare a statement of strategic priorities which the ICO must have regard to when discharging its functions?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

<u>The ICO's international role</u>

347. The ICO plays a crucial role in promoting responsible cross-border data flows - for example through its work on developing and maintaining transfer tools, such as standard contractual clauses (SCC) and binding corporate rules (BCR), and its influential regulatory cooperation activities in key global regulatory for a such as the Global Privacy Assembly and OECD Working Group on Data Governance and Privacy, both of which the ICO chairs. Although the ICO has a legislative mandate to conduct this work, the government believes its international role could benefit from clearer strategic objectives against which it can prioritise its activities and resources, evaluate its performance and be held accountable by its stakeholders.

[94] Digital Economic Act 2017, s.98
[95] Energy Act 2013, c.23
[96] Water Industry Act 1991, c.51

348. **The government proposes that the ICO should deliver a more transparent and structured international strategy, as part of its accountability and transparency requirements.**

349. **The government also proposes to include, as part of the new framework of objectives and duties, a new statutory objective for the ICO to consider the government's wider international priorities when prioritising and conducting its own international activities.** While the ICO's responsibilities and powers with respect to transfer tools and regulatory cooperation are provided for under Articles 57 and 50 in the UK GDPR respectively, the proposed international objective would help the ICO prioritise its activities in light of its expanding remit in these areas following the UK's exit from the European Union.

350. These proposals align with the Plan for Digital Regulation and are guided by the principle of exploiting opportunities and addressing challenges in the international arena. This will ensure that the ICO is able to build international considerations from the start, taking account of the government's international obligations and the impacts of regulations developed by other nations.

The government welcomes views on the following questions:

Q5.2.12. To what extent do you agree with the proposal to require the ICO to deliver a more transparent and structured international strategy?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q5.2.13. To what extent do you agree with the proposal to include a new statutory objective for the ICO to consider the government's wider international priorities when conducting its international activities?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

5.3 Governance Model and Leadership

351. The ICO's governance and leadership model should be fit for purpose, suitable to its role and remit, and relevant to the rapidly evolving regulatory landscape. The ICO also needs the right governance structures in place to deliver its ongoing transformation programme, building the capability and processes necessary to regulate effectively in an increasingly data-driven world. It is crucial the ICO has the right expertise and skills at the top of the organisation to make this transformational change a success.

352. The ICO is currently structured as a 'corporation sole'; a single legal entity consisting of an incorporated office occupied by a single person. The powers and responsibilities of the ICO lie solely with the Information Commissioner. Most peer regulators of the ICO in the UK run a governance board model, including a separate, statutory independent board function which

provides direction to - and scrutiny of - the executive function of the organisation. In contrast, a corporation sole is run by the executive function, without a chair or statutory independent board. A corporation sole model makes the ICO an outlier for a large regulator with a broad and important remit. This model can lead to a lack of diversity, challenge and scrutiny that is critical to robust governance and decision-making.

353. **To address the risks above, the government proposes to establish an independent board and a chief executive officer at the ICO.** The board would be led by a chair with non-executive directors. The chief executive officer would have responsibility for the running of the organisation, while answering to the board.

354. The establishment of an independent chair and statutory board will formalise aspects of the ICO's existing governance arrangements. Some of the Information Commissioner's responsibilities are already delegated to others - for example, the setting and oversight of the ICO's strategic direction is delegated to the ICO Management Board, and administrative and regulatory leadership is delegated to its Executive Team. Despite the opportunity for some delegation in practice, the formal concentration of responsibilities and powers in a single individual means that there is still the potential for a lack of resilience and continuity in leadership at the ICO. Constituting a new governance model formally in legislation will create greater clarity and certainty, and allows for the appropriate public appointment processes by the government that are commonplace for UK regulators.

355. This model is considered best practice for regulators in the UK, such as Ofcom and the Financial Conduct Authority, and across OECD countries, delivering reliable decision-making owing to more collegiality, and a greater level of independence and integrity.

356. The role of UK Information Commissioner is recognised and valued both domestically and internationally. It is important to preserve this brand and reputation under the new model. The government intends for the title of 'Information Commissioner' to be attached to the role of chair under the new model.

The government welcomes views on the following question:

Q5.3.1. To what extent d*o you agree that the ICO would benefit from a new governance and leadership model, as set out above?*

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Appointments processes

357. The current appointments process for the Information Commissioner is transparent and well-respected, balancing the importance of the ICO's independence with appropriate oversight by the government and Parliament.

358. **The government proposes to appoint the chair by the same process as that currently set out for the appointment of the Information Commissioner in the Data Protection Act 2018.** This means that the chair will be appointed by Her Majesty by Letters Patent, following a recommendation from the government based on merit, following a fair and open competition.

359. The government recognises the importance of having the right skills and experience in senior roles at the ICO. The current Public Appointment process for the Information Commissioner sets a valuable benchmark. **The government proposes that the individual non-executive members of the ICO's future board and its chief executive officer role will also be appointed via the Public Appointment process.** Government ministers are responsible and accountable to Parliament for public appointments and all appointments follow a recruitment process set out in the Governance Code for Public Appointments, regulated by the Commissioner for Public Appointments.

The government welcomes views on the following questions:

Q5.3.2. To what extent do you agree with the use of the Public Appointment process for the new chair of the ICO?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q.5.3.3. To what extent do you agree with the use of the Public Appointment process for the non-executive members of the ICO's board?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q5.3.4. To what extent do you agree with the use of the Public Appointment process for the new CEO of the ICO?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

360. Clarity and transparency around the scope and role of the ICO's future board, such as where key decisions are made and the delineation of responsibilities, should be set out in a corporate

governance framework. This will include effective governance mechanisms for the ICO's freedom of information responsibilities.

Setting the Information Commissioner's salary

361. The current legislation requires Parliamentary approval to amend the Information Commissioner's salary. Given the government's planned changes to the ICO's governance model, the provision for Parliament to set the chair's salary would become an outlier compared to other regulators.

362. **The government proposes to remove the requirement for Parliamentary approval and allow the Secretary of State for DCMS to amend the Information Commissioner's salary with approval from HM Treasury.** Safeguards exist within this process and salaries over £150,000 are governed by HM Treasury's Guidance for approval of senior pay, which sets out that sponsor departments must have regard to ensuring value for money and ensuring they can recruit, retain and motivate the best people.

The government welcomes views on the following questions:

Q5.3.5. To what extent do you agree that the salary for the Information Commissioner (i.e. the proposed chair of the ICO in the future governance model) should not require Parliamentary approval?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

5.4 Accountability and Transparency

363. The changes to the ICO's statutory framework for objectives and duties, coupled with stronger governance mechanisms, as set out above, will improve the diversity, challenge and scrutiny of the ICO's approach within the organisation itself. Furthermore the government intends to strengthen accountability and transparency mechanisms in order to aid external scrutiny of the ICO's performance.

364. The proposed accountability and transparency changes relate to the ICO's entire remit. The government has taken into account the ICO's independence and regulatory oversight of the public sector when considering these changes in order to uphold the ICO's independence while ensuring it can be effectively held accountable for its activities.

New reporting requirements

365. The ICO is currently required to produce, lay before Parliament and publish a general report, including its annual report.[97] However, as highlighted earlier in this chapter, there is a lack of clarity around the ICO's strategic priorities in the current legislative framework, meaning there are no clear objectives for the ICO to measure its performance against and report on.

[97] Data Protection Act 2018, Section 139

366. **The government proposes to introduce a requirement for the ICO to develop and publish comprehensive and meaningful key performance indicators (KPIs) to underpin its annual report.** The KPIs and the annual report should be underpinned by robust monitoring and evaluation of the ICO's activities.

367. In order to ensure Parliament and the government, regulated entities, the public and civil society hold the ICO to account effectively, it is important that various pieces of evidence and information are included in the KPIs and annual report as a basis for determining how effectively the ICO is discharging its functions. The intention is to enhance the regulator's accountability by introducing defined reporting requirements, building on those already set out in law, such as the existing requirement on the ICO to provide guidance on how it exercises its enforcement function and penalties.[98]

368. The government is exploring whether to require mandatory reporting against the following:

    a. The proposed new overarching objective(s)

    b. The proposed growth and innovation duty, its competition duty and its duty to cooperate or consult with other regulators

    c. The proposed international objective(s)

    d. Its own objectives and goals as set out in its strategic documents

    e. The proposed strategic statement of priorities

    f. For investigations, the number of investigations undertaken, their nature, the time taken to complete the investigation and its outcome

369. Requiring the ICO to report how it is delivering against its objectives and duties will help to assure all interested parties that the ICO undertakes a robust approach to discharging its functions.

370. The ICO would continue to be subject to Parliamentary scrutiny via existing mechanisms, and the new overarching objective and duties would fall within the scope of the DCMS Select Committee, alongside the usual Parliamentary oversight and scrutiny processes.

371. **In addition to the requirements to develop KPIs, the government is exploring whether to mandate certain transparency requirements so that the ICO is required to publish the key strategies and processes that guide its work.** While a list in legislation is not envisaged, this requirement may cover documents that set out *what* the ICO does (i.e. its strategic plans and business plans) as well as *how* it carries out its functions (i.e. its Regulatory Policy Methodology Framework and its Regulatory Action Policy).

The government welcomes views on the following questions:

Q5.4.1. To what extent do you agree with the proposal to strengthen accountability mechanisms and improve transparency to aid external scrutiny of the ICO's performance?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*

[98] Data Protection Act 2018, Section 160

- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q5.4.2. To what extent do you agree with the proposal to introduce a requirement for the ICO to develop and publish comprehensive and meaningful key performance indicators (KPIs) to underpin its annual report?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q5.4.3. To what extent do you agree with the proposal to require the ICO to publish the key strategies and processes that guide its work?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q5.4.4. What, if any, further legislative or other measures with respect to reporting by the ICO would aid transparency and scrutiny of its performance?

- *Yes*
- *No*
- *Don't know*

Please explain your answer, and provide supporting evidence where possible.

Q5.4.5. Please share your views on any particular evidence or information the ICO ought to publish to form a strong basis for evaluating how it is discharging its functions, including with respect to its new duties outlined above.

Independent review

372. The reforms outlined above should drive considerable change in how the ICO monitors and reports on its activities. In certain circumstances, the government may wish to assess the ICO's performance independently. Currently, the government can conduct reviews of the ICO with the

agreement of the Information Commissioner but there is no mechanism that permits a fully independent review by a third party.

373. **The government proposes to empower the DCMS Secretary of State to initiate an independent review of the ICO's activities and performance.** Such a step may be taken if, for example, the ICO's performance were to slip below a threshold determined with reference to the enhanced accountability mechanisms set out above, or after prior notifications about shortcomings in performance. This would be comparable to, for example, HM Treasury's ability to instruct a review of the efficiency and effectiveness of the Financial Conduct Authority (FCA), as set out in the Financial Services Act 2012.[99]

The government welcomes views on the following questions:

Q5.4.6. To what extent do you agree with the proposal to empower the DCMS Secretary of State to initiate an independent review of the ICO's activities and performance?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q5.4.7. Please share your views on what, if any, criteria ought to be used to establish a threshold for the ICO's performance below which the government may initiate an independent review.

5.5 Codes of Practice and Guidance

374. Under the Data Protection Act 2018, the Information Commissioner is required to prepare codes of practice on four specified data processing activities in order to outline best-practice for organisations. The legislation also requires the Information Commissioner to consult the DCMS Secretary of State, and other parties considered appropriate, before preparing or amending three of the codes.[100] In addition, under its general functions, the Information Commissioner has powers to publish guidance on processing activities that relate to data protection.

375. The ICO now carries out impact assessments, and undertakes enhanced consultation with both government and other stakeholders when developing codes of practice, and complex or novel guidance. This approach is set out in the ICO's Regulatory Policy Methodology Framework.

376. **The government proposes to oblige the ICO to undertake and publish impact assessments, as well as conduct enhanced consultation, when developing codes of practice, and complex or novel guidance.** This will give the current processes a statutory underpinning.

[99] Financial Services Act 2012, 1S, c. 21, PART 2, 'Financial Conduct Authority and Prudential Regulation Authority'.
[100] The data-sharing, direct marketing, age-appropriate design code.

377. Although the ICO has taken steps to produce 'at a glance' guides and sector-specific toolkits to assist smaller organisations, its core guidance may be very lengthy. It is crucial that the ICO's codes of practice and guidance are accessible and enable regulated entities to comply with the legislation efficiently and easily.

378. A robust consultation process is critical to this, particularly in relation to codes of practice or guidance which relate to more complex areas of legislation. As the ICO is a cross-sector regulator, a broad and transparent consultation process could improve the ICO's understanding of how legislation should apply to different sectors and data use cases, its focus on the most relevant issues, and its production of bespoke products for certain groups or organisations, such as SMEs.

379. **To encourage diverse debate, the government proposes to introduce a power for the DCMS Secretary of State to require the ICO to set up a panel of persons with relevant expertise when developing codes of practice, and complex or novel guidance.** Such a process would not be feasible or proportionate for the development of every piece of guidance, hence its limitation to statutory codes, or complex and novel guidance. The ICO should select experts so that the panel is, as far as possible, representative of the primarily affected groups in the given context. The ICO will be required to explain, as part of its regulatory approach, its process and rationale for appointing expert panels. The ICO must publish the outcomes of the panel's work, although it will not be bound by any recommendations of the panel.

380. **Furthermore, the government proposes to give the Secretary of State for DCMS a parallel power to that afforded to the Houses of Parliament in section 125(3) of the Data Protection Act 2018 in the approval of codes of practice and complex or novel guidance.**[101] This will give the Secretary of State a 40-day period to approve a code of practice or complex or novel guidance. If the Secretary of State does not approve it, the ICO must not issue it and another version must be prepared.

The government welcomes views on the following questions:

Q5.5.1. To what extent do you agree with the proposal to oblige the ICO to undertake and publish impact assessments when developing codes of practice, and complex or novel guidance?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q5.5.2. To what extent do you agree with the proposal to give the Secretary of State the power to require the ICO to set up a panel of persons with expertise when developing codes of practice and complex or novel guidance?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*

[101] Data Protection Act 2018, Section 135(3)

- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q5.5.3. To what extent do you agree with the proposal to give the Secretary of State a parallel provision to that afforded to Houses of Parliament in Section 125(3) of the Data Protection Act 2018 in the approval of codes of practice, and complex and novel guidance?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q5.5.4. The proposals under this section would apply to the ICO's codes of practice, and complex or novel guidance only. To what extent do you think these proposals should apply to a broader set of the ICO's regulatory products?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and describe alternative or supplementary criteria if appropriate.

Q5.5.5 Should the ICO be required to undertake and publish an impact assessment on each and every guidance product?

- *Yes*
- *No*
- *Don't know*

Please explain your answer, and provide supporting evidence where possible.

5.6 Complaints

381. Current legislation requires the ICO to allocate a significant amount of its resources to handling data protection complaints; some of this activity delivers low-value outcomes for data subjects and is poor value-for-money for data protection fee payers.[102] The government wants to create a more efficient and effective model that delivers better outcomes for overall public trust by

[102] Information Commissioner's Annual Report and Financial Statements 2019-20, p.47

enabling the ICO to take a risk-based approach, focusing on upstream activities in order to identify and address problems before they cause widespread harm.

382. The ICO currently allocates a significant proportion of its resources to handling a high volume of enquiries and complaints from the general public about data protection. In 2020/21 the ICO received 36,607 new complaints, only a slight decrease from the 38,514 in 2019/20 and more than they received in 2018/19.[103]

383. Under UK GDPR and the Data Protection Act 2018, there is currently no threshold to make a complaint to the ICO.[104] Internationally, this contrasts with other regimes such as the New Zealand Privacy Act (2020) which, whilst enshrining the right of data subjects to complain to the Commissioner, also provides guidelines outlining why the Commissioner may decide not to investigate a given complaint, including if the complainant has not made reasonable efforts to resolve the complaint directly with the data controller first.[105]

384. **The government proposes introducing a requirement for the complainant to attempt to resolve their complaint directly with the relevant data controller before lodging a complaint with the ICO.** This would encourage better explanation and more dialogue between data subject and data controller, prior to the complaint reaching the stage of an ICO investigation. It would also help to reduce the number of vexatious complaints if data subjects are required to resolve issues with the data controller before complaining to the regulator. Moreover, it would bring the ICO into line with other domestic ombudsmen and regulatory bodies such as Financial Ombudsman Services, which require complainants to lodge a complaint with the organisation or service provider before lodging a formal complaint with the ombudsman.

385. There would need to be guidance and exemptions in place in certain circumstances that allow the data subject to proceed directly to the ICO with their complaint; for example, following a period of undue delay from the controller, or in the context of complaints from or involving children or vulnerable people.

386. **To complement this new obligation on data subjects, the government is also proposing a requirement on data controllers to have a simple and transparent complaints-handling process in place to deal with data subject complaints.** This is not mandatory under the current data protection regime. This is in contrast to countries such as Singapore, which require controllers to develop a process to receive and respond to data protection complaints and make information about their policies and practices available.[106] We would require data controllers to be more transparent by asking them to publish information about the type and volume of complaints they receive on a periodic basis, although this would need to be accompanied by exemptions to avoid burdening SMEs or organisations that process data in a low risk way. This requirement would likely form part of the proposed 'privacy management programme' (PMP) for organisations, set out in Chapter 2 above.

387. **To further reduce the burden on the ICO, the government is also exploring whether to introduce criteria by which the ICO can decide not to investigate a given complaint.** Under

[103] InformationCommissioner's Annual Report and Financial Statements 2020/21, p.36
[104] Part 6, para 165 of the Act states: 'Articles 57(1)(f) and (2) and 77 of the UK GDPR confer rights on data subjects to complain to the Commissioner if the data subject considers that, in connection with personal data relating to him or her, there is an infringement of UK GDPR.'
[105] Privacy Act 2020 No 31 (as at 01 April 2021), Public Act 74 Commissioner may decide not to investigate complaint – New Zealand Legislation
[106] See Part III, Para. 12 of the Singaporean Personal Data Protection Act (2012)

the current legislation, the ICO has some flexibility about the extent to which they investigate complaints: the legislation states that the Commissioner must investigate the subject matter of the complaint to the extent appropriate. Greater clarity in the legislation would allow the ICO to exercise discretion with greater confidence, and the ICO would be freed up to focus on complaints that carry a higher risk of harm to individuals. This would allow the ICO to investigate complaints in a more agile, risk-based way. The ICO's guidance on complaints already sets out the criteria it uses to determine whether to pursue a complaint, including the severity of the potential breach, how the data controller has dealt with any related concern, and the overall context.[107] Similarly, the New Zealand Privacy Act (section 74) provides an example of this approach internationally.

The government welcomes views on the following questions:

Q5.6.1. To what extent do you agree that the ICO would benefit from a more proportionate regulatory approach to data protection complaints?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q5.6.2. To what extent do you agree with the proposal to introduce a requirement for the complainant to attempt to resolve their complaint directly with the relevant data controller prior to lodging a complaint with the ICO?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q5.6.3. To what extent do you agree with the proposal to require data controllers to have a simple and transparent complaints-handling process to deal with data subjects' complaints?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

[107] ICO, 'A guide for data controllers',

Please also indicate what categories of data controllers, if any, you would expect to be exempt from such a requirement.

Q5.6.4. To what extent do you agree with the proposal to set out in legislation the criteria that the ICO can use to determine whether to pursue a complaint in order to provide clarity and enable the ICO to take a more risk-based and proportionate approach to complaints?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

5.7 Enforcement Powers

388. The ICO is responsible for monitoring and enforcing the UK data protection regime. The ICO should be a strong, effective regulator that is equipped with the powers it needs to investigate compliance with the legislation and take appropriate action, where necessary, when organisations and individuals undertake unlawful data processing.

389. When organisations are using personal data unlawfully, the ICO should have the right powers available to enforce the law and take action against the genuinely bad players. The enforcement framework set out in UK GDPR and Data Protection Act 2018 provides a robust set of tools for the ICO to achieve this. This includes a suite of enforcement tools ranging from information notices, which simply require organisations to provide specific information to the ICO, through to the ability to leverage fines up to £17.5 million, or 4% of total worldwide annual turnover, whichever is higher. The aim of the enforcement regime is to promote compliance and act in a robust and proportionate manner.

390. The table below summarises the ICO's existing enforcement powers:

Power and Statutory basis	Scope
Monitor and enforce UK GDPR, including conducting **investigations** GDPR, Art.57	The Information Commissioner's duties to monitor and enforce the UK GDPR and to conduct investigations.
Information Notice Data Protection Act s.142-144	The ICO can serve an information notice on a controller or processor to request provision of information reasonably required to help the ICO carry out its statutory functions. A notice may also be served on any other person to help investigate suspected failure to comply with a Specified Failure of the UK GDPR, Data Protection Act 2018 etc (as defined below). The

Power and Statutory basis	Scope
	information set out in the notice must be provided to the ICO within the specified period in the notice.
Information Order Data Protection Act s.145, UK GDPR Art.57	The ICO can apply to the courts to issue a formal order requiring compliance with an information notice.
Assessment Notice Data Protection Act s.146-147	The ICO can serve an assessment notice on a controller or processor requiring them to permit the ICO to carry out an assessment as to whether they are complying with the data protection legislation. The notice may extend to allowing the ICO to access an organisation's sites and premises, view information held on the premises, observe processing activities etc. In certain situations, the ICO can also carry out no-notice inspections.
Enforcement Notice Data Protection Act s.149-153	The ICO can serve an enforcement notice on a controller or processor for failure to comply with specified provisions in the UK GDPR / Data Protection Act 2018; a Code of Conduct; or the fees regulations ("**Specified Failures**"). The notice may require the organisation to either take or refrain from taking certain actions in order to address the Specified Failure.
Penalties Data Protection Act Schedule 16	The ICO can serve a monetary penalty notice for a Specified Failure, or failure to comply with an information notice, assessment notice or enforcement notice. Penalties may extend up to £17.5 m or 4% of annual global turnover, whichever is higher. Before issuing a penalty, the ICO must, by written notice ("notice of intent") inform the person that they intend to give a penalty notice. The notice also states the person may make written representations and specifies the period within which such representations may be made.

391. We consider the current enforcement provisions to be broadly fit for purpose; the regulator has tools appropriate to both promote compliance and to impose robust, proportionate and dissuasive sanctions where necessary.

The government welcomes views on the following question:

Q5.7.1. To what extent do you agree that current enforcement provisions are broadly fit for purpose and that the ICO has the appropriate tools to both promote compliance and to impose robust, proportionate and dissuasive sanctions where necessary?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

392. We are, however, exploring three areas where the ICO's powers may need to be extended in limited circumstances.

A power to commission technical reports

393. During the course of its investigations into suspected infringements of the data protection regime, the ICO has, in some cases, faced challenges in receiving timely and sufficiently detailed information from organisations regarding the technical and organisational measures it has in place at the time and any remedial measures going forward. It is thought that some organisations have also sought to manage the content of such information to limit the degree by which they expose internal failings and any other vulnerabilities identified.

394. **The government is therefore proposing to introduce a new power for the ICO to be able to commission an independently-produced technical report to inform investigations to obtain a view from a third party about aspects of a regulated organisation's activities.** This would be similar to the power the Financial Conduct Authority (FCA) has under the Financial Services and Market Act (s.166). Examples of when such a power would be used are: if there are concerns as to whether the organisation being investigated is sharing the full scope of relevant information; where there are concerns that the organisation has not obtained sufficiently detailed information following a breach; or, where there is a need for further analysis of the technical measures already in place and any remedial measures required to mitigate future risks of harm or detriment to data subjects.

395. It is envisaged that this power would only be used in a small minority of investigations, likely to be those that are particularly complex and technical in nature or where there is significant risk of harm or detriment to data subjects. Thresholds will be put in place to ensure the use of such a power is evaluated at a case by case level and limited to appropriate circumstances. Furthermore, we intend to stipulate that consideration is given to the relevant organisation's financial circumstances.

396. The reports will be shared with the ICO and the organisation in question, which will enable them to better understand weaknesses in their systems and how to improve them. External expert analysis of a technical nature will result in more informed investigations which will ultimately mean better enforcement and enhanced data security/cyber hygiene by the organisation. Where cases are subject to appeal, it could also help reduce disagreements concerning the facts of the case.

Case study: ***Data breach where a technical report would improve outcomes***

A data controller had their remote access systems compromised through employee credentials being gained by the attacker. Once the attacker logged into the main network, the attacker exfiltrated data and encrypted the systems, impacting a large amount of personal data related to both customers and employees.

The data controller recognised the means of attack as compromising remote access credentials, and the steps taken by the attacker to deploy ransomware, and determined that the best mitigation to the incident was to reset their remote access credentials to prevent a future attack and deploy backups to enable data recovery. The organisation did not commission its own technical report.

Although these remedial measures were correct and vital for the organisation to complete, this makes an assumption that what the attacker did and what the attacker could have done are the same thing. This therefore raises questions such as:

- If ransomware was not deployed and a different attack was chosen by the attacker, would the access to the network have been detected?
- What methodology was used to exfiltrate data from the network? Can the organisation be certain what personal data was compromised?
- What actions could the attacker have taken once they managed to log into the network and how can the organisation be certain the attacker is not still 'in' its systems?
- What are the possible actions that could have led to the compromised credentials, and how can we prevent this from occurring?

Missing these questions creates a large risk for the organisation. Not only that a future attack could occur, but that it could be significantly worse if the attacker chooses to perform further reconnaissance, maintains a presence in the system for longer and performs a more bespoke attack against the network.

During an ICO investigation, the provision of a technical report would provide an external assessment of incident detection, security incident monitoring systems, exfiltration methodology (how the attacker was able to steal personal data) and how the employee's credentials were compromised. The absence of a technical report in such circumstances would mean the ICO would be unlikely to be able to make an accurate determination of the risk involved in the breach, the potential harm this could cause individuals (those whose personal data has been stolen) and the adequacy of the measures taken by the data controller.

The government welcomes views on the following questions:

Q5.7.2. To what extent do you agree with the proposal to introduce a new power to allow the ICO to commission technical reports to inform investigations?

- *Strongly agree*
- *Somewhat agree*

- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible, including:

- *Whether there are any other risks or benefits you can see in this proposal*
- *If you foresee any risks, what safeguards should be put in place*

Q5.7.3. Who should bear the cost of the technical reports: the organisation (provided due regard is made to their financial circumstances) or the ICO?

Q5.7.4. If the organisation is to pay, what would an appropriate threshold be for exempting them from paying this cost?

A power to compel witnesses to answer questions at interview

397. The ICO is obligated to monitor and enforce the UK's data protection legislation (Article 57, UK GDPR) and to do this, the ICO should be able to hold organisations and individuals to account to establish all the relevant facts and, in particular, determine whether or not an organisation has failed to comply with what is required. Organisations have a duty to cooperate with the ICO (s.63, Data Protection Act 2018).

398. In the past, however, individuals have refused to fully cooperate with the ICO, for instance by declining to be interviewed as part of an investigation without prior reassurance that they would not be held accountable for any breach of the data protection framework, an assurance which the ICO could not give prior to having obtained their account.

399. **In order to clarify the scope of the ICO's investigatory powers, the government is exploring whether there is a need for a power which explicitly allows the ICO to compel witnesses to interview in the course of an investigation.** The ability to interview a relevant individual as part of an investigation could provide an important tool for gathering evidence - for example, unearthing information that may not be documented in written form. This would result in a more robust, detailed understanding of the case and assist with the correct interpretation of other evidence.

400. Enforcers' power to compel witnesses to attend an interview is not new. The Financial Conduct Authority can also compel relevant people to be interviewed during its investigations.[108]

401. As this is a wide-ranging power with implications on individuals' rights and freedoms, any consideration of the granting of this power needs to be carefully evaluated. Compelling witnesses to attend an interview will assist the ICO's enquiries and progress investigations at a faster pace,

[108] An investigator may require the person who is the subject of the investigation ("the person under investigation") or any person connected with the person under investigation (a) to attend before the investigator at a specified time and place and answer questions; or (b)otherwise to provide such information as the investigator may require. Financial Services and Market Act 2000, Section 171

which can be imperative during large scale complex investigations, and early evidence could limit the damage caused to data subjects.

402. The government will set clear parameters to ensure proportionate use of the power to compel a witness to interview to prevent its misuse or overuse. We propose the power applies only to individuals with a formal connection to the investigation; in most cases this would mean they are current or former employees of the organisation in question. Written notice to attend must be provided in advance and careful consideration must be given to the right not to self-incriminate.

403. The government is also considering whether to include a provision within this proposed power to compel the witness to answer questions on any matter relevant to the investigation. This is in order to ensure their cooperation with the investigation. If included, the government would include provisions to ensure its use respects an individual's rights and remains fair and proportionate.

The government welcomes views on the following questions:

Q5.7.5. To what extent do you agree with what the government is considering in relation to introducing a power which explicitly allows the ICO to be able to compel witnesses to attend an interview in the course of an investigation?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible. In particular, please give your views on any benefits or risks you envisage and what measures could mitigate these risks.

Q5.7.6. To what extent do you agree with extending the proposed power to compel a witness to attend an interview to explicitly allow the ICO to be able to compel witnesses to answer questions in the course of an investigation?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible. In particular, please give your views on:

- *Any benefits or risks you envisage*
- *What, if any, additional safeguards should be considered*

<u>Amending the statutory deadline for the ICO to issue a penalty following a Notice of Intent</u>

404. Schedule 16 paragraph 2(2) of the Data Protection Act 2018 sets out a six-month deadline between the ICO issuing a Notice of Intent and a final penalty notice.[109] At present, following an investigation into a suspected infringement of the regulations, the ICO issues a Notice of Intent setting out its case. The organisation in question then has the opportunity to make written representations and may also request to make oral representations. This needs to be completed within 28 days although an extension can be requested, if the organisation has reasonable grounds. The ICO has a responsibility to give due consideration to those representations before issuing a final decision notice. The final notice must be issued within six months of the Notice of Intent, unless there is mutual agreement for an extension. If it is not possible to conclude the investigation within this time or agree an extension, the ICO is prevented from issuing a penalty notice.

405. **The government is proposing an amendment to the statutory deadline for the ICO to issue a final penalty notice following a Notice of Intent from 6 months to 12 months.** The 6 months currently allowed was not updated when UK GDPR was introduced (so has remained unchanged since the Data Protection Act 1998) and does not reflect the increased complexity of some investigations or the increased maximum level of fines (which, on occasion, means organisations submit extensive written representations). Extending the time allowed would make it possible for the ICO to give organisations more time to respond to their enquiries and the ICO more time to take into account the range of evidence they present in their representations. By way of comparison, there is no deadline for the CMA to reach a decision on a final penalty.

406. **In the context of the amendment to the statutory deadline, the government is also proposing the inclusion of a so-called 'stop-the-clock' mechanism in Schedule 16(2) of the Data Protection Act 2018.** In the course of investigations, following receipt of the parties' representations, it may be necessary to gather further evidence in order to properly assess the representations. If the requested information is not provided on time, this can delay the ICO's assessment, potentially making even the extended timelines challenging and creating an incentive for companies to use delaying tactics. This amendment is analogous to the situation in mergers control, where the competition authority is subject to a statutory deadline and has the power to stop the clock if relevant information is not provided on time.

The government welcomes views on the following questions:

Q5.7.7. To what extent do you agree with the proposal to amend the statutory deadline for the ICO to issue a penalty following a Notice of Intent in order to remove unnecessary deadlines on the investigations process?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q5.7.8. To what extent do you agree with the proposal to include a 'stop-the-clock' mechanism if the requested information is not provided on time?

- *Strongly agree*

[109] Data Protection Act 2018, Section 16, Paragraph 2 (2)

- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Enhancing the ICO's accountability regarding investigations

407. In order to ensure that the ICO's investigations and any resulting enforcement action are conducted in a timely manner, the government is considering setting out further accountability requirements on the regulator.

408. **The government proposes placing a requirement on the ICO to set out anticipated timelines for the phases of an investigation to the relevant data controller(s) at the beginning of an investigation.** Provision would be made to allow the ICO to extend these timelines, particularly in response to changing circumstances if required.

The government welcomes views on the following question:

Q5.7.9. To what extent do you agree with the proposal to require the ICO to set out to the relevant data controller(s) at the beginning of an investigation the anticipated timelines for phases of its investigation?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

5.8 Biometrics Commissioner and Surveillance Camera Commissioner

409. We must continue to review and simplify the regulatory landscape and the functions of the ICO to avoid duplication, overlaps and lack of clarity. For example, the oversight arrangements for the police's use of biometrics and overt surveillance are crowded and confusing. The Biometrics Commissioner covers police use of DNA samples, DNS profiles and fingerprints, and the Surveillance Camera Commissioner covers all use of surveillance cameras by specified public authorities (including local authorities and the police), while the ICO covers the processing of all personal data by the public and the private sector in the UK.

410. The government recently simplified these arrangements by appointing one person to take on what were previously the part-time roles of Biometrics Commissioner and Surveillance Camera Commissioner. **The government will explore the potential for further simplifying the oversight framework by absorbing the functions of those commissioner roles into the ICO, which should bring benefits to data controllers and the public with a single route for advice, guidance and redress.**

The government welcomes views on the following questions:

Q5.8.1. To what extent do you agree that the oversight framework for the police's use of biometrics and overt surveillance, which currently includes the Biometrics Commissioner, the Surveillance Camera Commissioner and the ICO, could be simplified?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

Q5.8.2. To what extent do you agree that the functions of the Biometrics Commissioner and the Surveillance Camera Commissioner should be absorbed under a single oversight function exercised by the ICO?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.

5.9 Further Questions

Q5.9.1. In your view, which, if any, of the proposals in 'Reform of the Information Commissioner's Office' would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

Q5.9.2. In addition to any of the reforms already proposed in 'Reform of the Information Commissioner's Office' (or elsewhere in the consultation), what other reforms do you think would be helpful to improve the effectiveness of the ICO?

How to respond

Who are we seeking to consult

1. We are keen to hear from a representative cross section of society, ensuring diversity and inclusion, and the consultation has been designed in line with the government Consultation Principles and with due consideration to the Public Sector Equality Duty.

2. Given the focus of the consultation, we consider it to have particular relevance to:
    - Individuals
    - Start-ups and small businesses
    - Technology companies and data-driven or data-rich companies
    - Investors in technology and data-driven or data-rich companies
    - Civil society organisations focused on consumer rights, digital rights, privacy and data protection
    - Academics, and research and policy organisations with a particular interest in the role of data in the economy and society, or as data controllers in their own right
    - Organisations involved in international data standards, regulation, and governance
    - Law firms and other professional business services

3. This consultation is on a UK-wide basis: we welcome responses from organisations and individuals across the UK. Responses from organisations not based in the UK are also welcome.

How to respond

4. Thank you for your interest in responding to this consultation. The consultation will be open for 10 weeks to allow time for your consideration and response.

5. To help us analyse the responses, please use the online system wherever possible. Visit DCMS's online survey platform to submit your response. Email responses can be sent to DataReformConsultation@dcms.gov.uk.

6. Hard copy responses can be sent to:
    Domestic Data Protection team
    DCMS
    100 Parliament Street
    London
    SW1A 2BQ

7. If you are submitting a hard copy response, please submit by Friday 19 November. Please include details about the size of your organisation, or if you are responding as an individual, your interest in data reform and your profession.

Summary of next steps

8. The government's response to this consultation will be published in due course following its closure on 19 November 2021. This will take all responses submitted to this consultation into account, and will be based on careful consideration of the points made in responses.

Privacy notice

The following is to explain your rights and give you the information you are entitled to under the Data Protection Act 2018 and the UK General Data Protection Regulation ("the Data Protection Legislation"). This notice only refers to your personal data (e.g. your name, email address, and anything that could be used to identify you personally) not the content of your response to the consultation questions.

1. **What personal data does the Department for Digital, Culture, Media and Sport (DCMS) collect?**

Most of the personal information we collect and process is provided to us directly by you. This includes:

Personal identifiers, contacts and characteristics (for example, name and contact details).

2. **Why we are collecting your personal data**

Your personal data is being collected as an essential part of the consultation process, so that we can contact you regarding your response and for statistical purposes, such as to ensure individuals and organisations cannot complete the survey more than once.

3. **Our lawful ground for processing your personal data**

The Data Protection Legislation states that, as government departments, the departments may process personal data as necessary for the effective performance of a task carried out in the public interest (i.e. a consultation).

We will not:

- sell or rent your data to third parties
- share your data with third parties for marketing purposes
- use your data in analytics

We will share your data if we are required to do so by law – for example, by court order, or to prevent fraud or other crime.

4. **With whom we will be sharing your personal data**

Information you provide in response to this consultation, including personal information, may be disclosed in accordance with UK legislation (the Freedom of Information Act 2000, the Data Protection Act 2018 and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential please tell us but be aware that we cannot guarantee confidentiality in all circumstances.

We will summarise all responses and publish this summary on GOV.UK. The summary will include a list of names of organisations that responded, but not people's personal names, addresses or other contact details.

Qualtrics is the online survey platform used to submit responses to this consultation. They will store the data in accordance with the controller's instructions and their privacy policy.

5. **For how long we will keep your personal data, or criteria used to determine the retention period.**

Your personal data will be held for two years after the consultation is closed. This is so that the department is able to contact you regarding the result of the consultation, following analysis of the responses.

6. **Your rights, e.g. access, rectification, erasure**

The data we are collecting is your personal data, and you have considerable say over what happens to it. You have the right:

- to see what data we have about you
- to ask us to stop using your data, but keep it on record
- to have all or some of your data deleted or corrected
- to lodge a complaint with the independent Information Commissioner (ICO) if you think we are not handling your data fairly or in accordance with the law

You can contact the ICO at https://ico.org.uk, or phone 0303 123 1113. ICO, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

7. **Your personal data will not be used for any automated decision making**

8. **Your personal data will be stored in a secure government IT system and the survey company's secure system**

We are committed to doing all that we can to keep your data secure. We have set up systems and processes to prevent unauthorised access or disclosure of your data – for example, we protect your data using varying levels of encryption.

We also make sure that any third parties that we deal with keep all personal data they process on our behalf secure.

9. **Changes to this privacy notice**

We may change this privacy policy. In that case, the 'last updated' date at the bottom of this page will also change. Any changes to this privacy policy will apply to you and your data immediately.

If these changes affect how your personal data is processed, the controllers will take reasonable steps to let you know.

10. **What are your data protection rights?**

You have rights over your personal data under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). The Information Commissioner's Office (ICO) is the supervisory authority for data protection legislation, and maintains a full explanation of these rights on their website

DCMS will ensure that we uphold your rights when processing your personal data.

11. How do I complain?

The contact details for the data controller's Data Protection Officer (DPO) are:

Data Protection Officer
The Department for Digital, Culture, Media & Sport
100 Parliament Street
London
SW1A 2BQ
Email: DCMSdataprotection@dcms.gov.uk

If you're unhappy with the way we have handled your personal data and want to make a complaint, please write to the department's Data Protection Officer or the Data Protection Manager at the relevant agency. You can contact the department's Data Protection Officer using the details above.

12. How to contact the Information Commissioner's Office

If you believe that your personal data has been misused or mishandled, you may make a complaint to the Information Commissioner, who is an independent regulator. You may also contact them to seek independent advice about data protection, privacy and data sharing.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Website: www.ico.org.uk
Telephone: 0303 123 1113
Email: casework@ico.org.uk

Any complaint to the Information Commissioner is without prejudice to your right to seek redress through the courts.

This notice was last updated on 10/09/2021