Consultation outcome

Data: a new direction - government response to consultation

Updated 23 May 2022

Contents

About this consultation
Executive summary
Chapter 1: Reducing barriers to responsible innovation
Chapter 2: Reducing burdens businesses and society face when seeking to access personal data
Chapter 3: Governance and enforcing barriers to data flows
Chapter 4: Data adequacy, trade and security
Chapter 5: Reform of the Information Commissioner's Office
Questions on analysis of impacts
Public sector equality duty (PSED) assessment
Annex A: List of consultation responses
Annex B: List of organisations that responded to the consultation

Print this page

Introduction

The government launched its consultation 'Data: a new direction' on 10 September 2021 to seek to develop proposals for reform the UK's data protection laws, to secure a pro-growth and trusted data regime as part of the UK's National Data Strategy.

As the government set out in the National Data Strategy, personal data is a huge asset for the economy and society. It underpins innovation and trade, it is increasingly in business large and small, drives scientific discovery and has been lifeline during the global coronavirus pandemic. This government's ambition on data is to unleash the power of data across the economy and society for everyone.

We want to create a framework which empowers citizens through the responsible use of personal data. Our reforms will give individuals greater clarity over their rights and a more streamlined, less burdensome, data protection regime which means that organisations given confidence to innovate and use more medical breakthroughs creating better care for individuals. The UK's independent data protection regulator, the Information Commissioner's Office (ICO), will be more focused on protecting people from nuisance calls and attempts a source of crime but some of the most vulnerable in our society. These reforms will create a data rights regime which delivers not only economic benefits but wider societal benefits around people's quality of life.

The reforms we are taking forward will help the UK realise the benefits of greater innovation and trade. We want to ensure that the UK's data protection regime is responsible use of personal data. Big tech businesses the opportunity to protect personal data in the most proportionate and appropriate way, we will make them more accountable for the impacts of their data processing on society. We want to enable small businesses to use anonymised business data to develop new products and services and to grow their business or more productive. Higher growth activities they can further fuel economic growth.

The reforms proposed in the consultation provide an opportunity for the UK to redesign its approach to regulation outside of the EU, and seize opportunities with the new freedoms Brexit provides. The UK's data protection regime has been shaped by the EU to remove inappropriate barriers to the free movement of personal data between EU states, scientific collaboration and national security and law enforcement cooperation. We want to take back control of our data protection regime, to develop economic which support greater interoperability of regulatory frameworks, create and more stable principles for trusted government access to data. These areas of work are critical to the government's ambition for the UK to be a global leader in science and scientific institutions to undertake data collection, to ensure that the UK's research and international commitments on the free flow of data.

Our reforms will mean that UK scientists are supported by clear, proportionate, evidence-based data protection rules. We want to empower personal data, we provide scientists with the clarity and confidence they need to get on with life-enhancing and life-saving research. We want to ensure that the data protection regime which our scientists use and to their strengths. Having legal clarity and certainty over what can do means they can spend more effort and resources into innovating. Indeed, our reforms will ensure that the UK's data protection regime is more supportive to new funds, further boosting the UK's research sector.

About the consultation

The current UK data protection regime consists of the UK General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications Regulations (PECR) and the Data Protection Act 2018 (DPA 2018). The government consulted on proposals for reform of the UK's current regime, such as to decrease unnecessary data rights for citizens, and its mechanisms for supervision and enforcement.

We are committed to maintaining these important principles:

- We will ensure that high standards of data protection and the UK's adequacy arrangements underpin our future data protection regime. The use of personal data will continue to be at the heart of our regime, while providing greater flexibility to organisations to find the most effective and proportionate way of protecting people's personal data.
- The UK's data protection regime will be future-proofed, by enabling organisations to take advantage of new technologies and other data methods - important privacy outcomes - rather than finding loopholes. This will enable our laws to keep pace with changes to the technological landscape without disrupting regulatory certainty.
- Almost all organisations that comply with the UK's current regime will continue to do so under our reforms. We want to make improvements to aim things that are already good in best practice and that many businesses already have in place.
- The UK's data protection regime will deliver concrete advantages for the UK while preserving data subjects' rights and the independence of our regulator, creating a net benefit for businesses and society as a whole.
- The reforms to the ICO will ensure effective, risk-based and proportionate supervision, improving the governance, accountability and transparency in line with best regulatory practice.

This consultation ran for 10 weeks, closing on 19 November 2021. The consultation received 1,108 responses from a wide range of UK and EU based organisations. Responses were received from the Information Commissioner's Office and organisations which represent a cross-section of the UK economy and society, as well as from overseas organisations.

During the consultation period, the government engaged with a range of stakeholders, including data protection officers, data ethics and AI ethics bodies, and consumer rights groups, providing a wide range of views.

This document is the government's response to the 'Data: a new direction' consultation.

Executive summary

The proposals in this response are arranged into 50 headings across 5 chapters:

- **Reducing barriers to responsible innovation**: Chapter 1 relates to providing clarity and certainty to businesses on the interpretation of current data definitions and requirements relating to personal data processing. The government's proposals in this chapter include: clarifying the UK's approach to increase confidence in personal data processing through use of the legitimate interest ground and enabling greater personal data access and personal data sharing for scientific research purposes. The government also proposes reforms to create more certainty for organisations about when and how they can responsibly use personal data with the development of cutting-edge data-driven technologies.
- **Reducing burdens on businesses and bolstering better outcomes for people**: Chapter 2 relates to reducing unnecessary burdens on organisations while bolstering better outcomes for people in relation to the processing of personal data. The corresponding chapter in the consultation paper contained a range of reforms to include: a new lawful ground for processing personal data for certain rights. This will strengthen accountability requirements while providing organisations with the opportunity and flexibility to find the most effective and proportionate way of protecting people's personal data and their data rights. It also included reforms to reduce disproportionate impacts of subject access requests on organisations, and reuse to limit unnecessary cookie banners by allowing users to the Privacy and Electronic Communications Regulations.
- **Boosting trade and reducing barriers to data flows**: Chapter 3 relates to boosting international data transfers and trade. The corresponding chapter in the consultation paper contained a range of reforms to include: autonomous UK international frameworks regime, which supports international trade and eliminates unnecessary obstacles to cross-border personal data flows.
- **Delivering better public services**: Chapter 4 relates to delivering better public services through better use of personal data across the economy. The corresponding chapter in the consultation paper contained proposals to make better use of data sharing gateways under the Digital Economy Act to facilitate more joined-up, evidence-based, data-driven government policies. This would also include transparency of government processing activities by ensuring that clear information is presented on the use of algorithms, and, simply the legal framework in relation to the public's data collection, use and retention of biometric data.
- **Reform of the Information Commissioner's Office**: Chapter 5 relates to the reform of the ICO, the UK's independent data protection regulator. The corresponding chapter in the consultation paper contained proposals to ensure the ICO is more accountable for its strategic direction and operations and require the ICO to account for the impacts of its activities on growth, innovation and competition.

Summary of responses

Overall, responses indicated support for the government's proposals in many areas, including:

- changes to research provisions, especially the proposal to consolidate and bring together research provisions, including the definition of scientific research purposes, research and the changes proposed to notification requirements
- removal of consent requirements in relation to audience measurement cookies
- the proposed approach to PECR enforcement, including aligning civil penalties across Adequacy and Alternative Transfer Mechanisms (ATMs)
- reforming the ICO, and emphasis on the importance of maintaining its regulatory independence
- standardising the terminology and definitions used across the data processing framework
- increasing clarity and transparency of the existing rules on police collection, use and retention of data for biometrics, in order to improve transparency and public safety
- the proposed approach to ATMs, and the approach to UK GDPR Article 49 international transfers, as this could be beneficial in terms of promoting public services.

There were some potential concerns raised about:

- introducing a minimum fee for subject access requests
- whether the government should have a role enabling the activity of responsible data intermediaries
- removing the need for data controllers to conduct a fair and balanced interests balancing test for specified activities if children's data were involved
- removing the right to human review of automated decisions
- whether to exclude political parties and charities from rules on direct electronic marketing
- removing requirements for Data Protection Impact Assessments (DPIAs) and Data Protection Officers (DPOs)
- the potential impact of reforms on the ICO's independence

As well as the policy specific feedback, several themes emerged consistently across all chapters of the consultation. These were: the need for clarity, the importance of the detailed discussion of areas in each of these areas can be found in the relevant chapters of this document.

Respondents highlighted the importance of maintaining data subject rights. The government agrees with the importance of maintaining data subject rights and the importance of maintaining high standards of data protection, as set out in the General Data Protection Regulation (UK GDPR), such as: its data processing principles, its data rights for citizens, and its mechanisms for supervision and enforcement. The government also agrees with the importance of maintaining a high level of protection for people's personal data and control for individuals over how their data is used. This view also aligns with the government's position to ensure that data protection is a fundamental right and that people should be able to trust that protect personal data, so we can have even greater confidence that personal data is being used responsibly.

Respondents made clear the benefits they saw from the effective use of personal data across the economy and society, and highlighted the role that this has to play in growth. The government agrees with this position and we recognise the power of the effective use of personal data to drive innovation and boost the economy, while continuously protecting people's safety and privacy.

Respondents raised the importance of data flows with the EU, and how our reforms will affect this - in particular with respect to the UK's EU data adequacy decision. Many respondents recognised the benefits of the government's approach to data protection and international data transfers, including the benefits of expressing confidence for these reforms to be in line relevant to the EU General Data Protection Regulation (EU GDPR). As the government made clear in the consultation, the UK's data protection regime has been shaped by the EU to remove the UK's market EU adequacy as it designs a future regime. This will be underpinned by maintaining high data protection standards - now and in the future. Protecting the free flow of data with our EU partners is important to the UK, as it will help to sustain a high quality regime that promotes growth and innovation, and underpins the trustworthy use of data. EU adequacy decisions do not require an 'adequate' regime to be identical to the EU's, but they do require a high standard of protection for personal data to compatible with maintaining flows of personal data without delays.

The consultation asked for views on a sliding scale of "strongly agree" through to "strongly disagree". While the quantitative figures are a useful indicator to understand the direction of travel of respondents, it should be noted that the ICO's response to nuance in terms of why respondents responded in a certain way, and can therefore not necessarily the best basis for assessing the relativities of the proposals. The qualitative responses provided by respondents have been very helpful in understanding and ensuring the complexity many were effectively balanced while delivering on the ambitious reform agenda.

Throughout this response when the opinions of respondents are referenced, this refers to those who chose to answer that specific question, which is not representative of the total number of respondents to the consultation or necessarily the UK public.

The remainder of this document sets out the government's response to the consultation in more detail, including its planned next steps in each area. As announced in the DCMS Business Plan 2022, DCMS will introduce a data protection reform legislation to reform the UK's data protection regime.

Chapter 1: Reducing barriers to responsible innovation

1.1 Summary

In chapter 1 of the consultation, the government highlighted the importance of innovation, responsible uses of personal data to help drive scientific discovery, enable better healthcare and better services for people across the economy.

Clear and consistent rules for the use of personal data will support the adoption of new data-driven technologies. The government's proposed reforms are designed to create more certainty for organisations about when and how they can responsibly use personal data, an important step in ensuring our laws protect people while supporting cutting-edge data-driven technologies. The development and deployment of data-driven technologies can have significant implications for people and society. These technologies will make businesses more efficient, and thus more productive, and these benefits will be felt by British consumers, through new innovative products, more jobs or lower prices.

1.2 Research purposes

The UK is ranked second in the world for science and research, and 81% of our research output is world leading. Personal data lies at the heart of a wide range of research activities across many sectors, and the importance of personal data to research activities is our economy and wider society is reflected in the UK GDPR.

The existing legislation already has specific provisions and derogations for facilitate research using personal data. The UK GDPR provides a lawful ground for processing for research purposes per consent, and the research exemption can also be used to allow personal data to be used for research purposes without consent. The research exemption is a flexible provision, it can be used to allow research to be carried out by researchers. Around a third of respondents agreed that Recital 159 was a suitable basis, on the grounds that it provided a clear and broad base that was understanded by researchers. Around a third of respondents disagreed that the current definition is too vague, and a similar proportion did not have a view.

Moving the definition from the recitals to the operative text of the UK GDPR will provide greater clarity and flexibility to both researchers and data controllers. It will also ensure that the definition remains future-proofed in addition. The government will also consider suitable ways to do this as research is a constantly evolving field and maintaining a definition in the recitals would allow for this. The government will also consider how to ensure that the definition remains future-proofed in addition. The government will also add the definitions for historic research and statistical purposes to the legislation alongside that for scientific research, to provide consistency and clarity across the fields of research currently recognised in the legislation.

Consolidating research provisions (question 1.3):

The government proposed consolidating and bringing together research specific provisions in the UK GDPR into a single section to improve clarity and ease of use. This would increase the clarity of the legislation, with some respondents noting that they were welcoming further guidance on this from the ICO. There was some disagreement with the proposal, with some respondents noting that the current provisions are clear and noting that consolidating them would be confusing from the ICO or that the current framework was sufficiently clear.

The ICO has recently launched a consultation on guidance about data processing for research. The draft guidance provides a detailed interpretation of the current research provisions. This guidance based approach governance based approach supports businesses and organisations to understand their data protection obligations. This approach is more targeted approach to simplifying the legislation by only making certain sections of the legislation rather than creating an entire chapter.

Lawful basis for research purposes (questions 1.4, 1.5, 1.6, 1.7, 1.8):

The government sought views on clarifications faced by scientific researchers trying to rely on consent as a lawful basis for data processing. The UK GDPR provides a clear and separate lawful basis for research. The majority of respondents agreed that identifying the most appropriate lawful basis did not create barriers to research.

There were mixed views regarding whether to create a new lawful basis for research purposes, with supportive respondents noting that a new lawful basis would help researchers navigate the data protection regime, and would increase confidence. Respondents who disagreed with the proposal argued this could be open to misuse, especially in conjunction with the broad definition for scientific research currently contained in Recital 159.

The government does not see a need to take forward proposals that would create a new lawful basis for research at this time, as the evidence suggests that researchers are currently comfortable in using the existing lawful bases for processing personal data.

Clarifying the use of broad consent (question 1.3.8):

There were mixed views on clarifying the use of broad consent, which allows scientific research to use a less specific form of consent when it is not possible to fully identify the purpose of personal data at the time of data collection. Some respondents welcoming the flexibility, innovation and clarity this would provide. Respondents who disagreed with the proposed cited concerns that it could be open to misuse, and that it is too broad.

It was also noted that, likely due to its location in the recitals, some respondents were not currently aware that broad consent is already a concept in the UK GDPR. The government will look at ways to improve clarity and certainty and encourage its use relative to broad consent in this context.

To help reduce uncertainty and concerns around misuse, as well as to improve awareness of broad consent's potential and use among organisations and individuals, the government will seek to make the provisions concerning broad consent in the recitals more prominent by putting them on the face of the legislation.

Clarifying the rules on further processing (question 1.3.9):

The UK GDPR provides a lawful basis for processing personal data for reusing rules on re-use for further processing of personal data for research, including the establishment of a lawful basis. Around a third disagree. As with broad consent, some of those opposed cited concerns around misuse, and that it is too broad. Some noted that organisations may use personal data in unexpected ways under the guise of research. However, those in favour saw the benefits of adding clarity to further processing.

As outlined in the consultation, a new lawful basis for research purposes does not see the need to take forward proposals to establish a lawful basis for research. This is in recognition of the fact that the UK GDPR already provides a clear and separate lawful basis for research purposes. However, to support transparency and clarity in the use for both organisations and individuals, the government will take forward wider proposals to clarify the rules on further processing. See further detail in the section on further processing (section 1.3).

Exemption to provide information regarding Article 13 (questions 1.3.10, 1.3.11):

The majority of respondents disagree with the proposal to introduce an exemption to the requirement for controllers to provide data subjects with the information required by Article 13 of the UK GDPR where personal data is collected from a source other than the data subjects and is to be used for research purposes, but only when providing the information required by Article 13 would involve disproportionate effort, and provided the controller has put in place appropriate safeguards. Respondents and organisations about individuals being control of their personal data. There is support of the measure argued that the information provision requirements in Article 13 are onerous and disproportionate, and that this could impede research and statistical studies. For instance, in studies about certain medical conditions (such as degenerative neurological conditions), researchers can hold a mix of directly collected and tracking data. Requiring researchers to provide fresh re-consenting, where it is impossible or very impossible to reconsent data subjects.

To ensure that research is not prevented in situations where reconsenting data subjects would be impossible or very difficult, the government will introduce a new exemption currently found in Article 14(5)(b), but only for research purposes. This change does not exempt controllers from providing all the relevant information in Article 13(1)&(2) to data subjects, it only exempts them from providing information about the source of being used for a research purpose which differs from the original purpose to be exempt from re-providing information under Article 13(3). It will only apply in circumstances where controllers can demonstrate disproportionate effort to the controller in providing such information.

The government will clarify what constitutes a disproportionate effort by bringing in language currently found in Recital 62 of the UK GDPR into the operative text. Alongside the existing ICO guidance in this area, this legislative change will provide clarity about when it is appropriate to use the exemption.

1.3 Further processing

As we (also known as "further processing") of personal data can provide economic and societal benefits, including for research purposes. The UK GDPR provides a clear and lawful basis for research purposes, but subjects broad in both transparency, data controllers benefit from certainty, and society benefits from unlocking the opportunities of re-use.

In recognition of the value of re-use of data in certain circumstances, the UK GDPR sets out a lawful basis for processing personal data for a purpose different to that for the purpose for which it was collected. In the consultation, the government identified areas of uncertainty and set out proposals to improve clarity in the legislation and thereby facilitate innovation in use of personal data and transparency for data subjects.

Clarify regarding further processing (question 1.3.1):

The UK GDPR provides a lawful basis for further processing in circumstances in further processing were confusing. There were also the legislation confusing explained by the uncertainty among organisations' compliance and legal teams regarding the rules on further processing. This has led to a risk averse approach to further processing innovation within their organisations. There were different interpretations from controllers and data subjects alike about whether further processing is currently lawful, and about what it means in practice. Many respondents to the consultation highlighting that they find the rules by a much clearer guide than the operative text.

The government judges that these responses are indicative of insufficient clarity in the current framework, and that there is a need for clarity. The government will clarify the legislation to address this, making it clear to organisations how personal data can be re-used for a purpose it is going to transparently to data subjects and individuals, and how it may be reused.

Clarifying further processing for an incompatible purpose when based on a law that safeguards important public interest (question 1.3.2):

The government sought views on various elements of further processing that cause difficulties in practice. Many respondents noted that the current provisions are unclear when based on a law that safeguards important public interest. There were mixed views regarding whether greater clarification was required. Some respondents expressed concerns about the ability to rely on consent, and about the ability to rely on compatibility test and whether it is always prohibited. However, this is permissible in certain cases under the current legislation.

In addition, the need for greater clarification on the rules and permissions of data re-use for further processing purposes. Therefore the government will proceed with this proposal.

Clarifying further processing when there has been a change of controller (question 1.3.3):

The government sought views on whether it would be beneficial to clarify whether or not a change of controller should be considered as further processing. The majority of respondents agreed that a change of controller should be considered as further processing. Around a third of respondents disagreed that clarification was necessary. Some respondents believed that if there is a change of controller, processing should be considered as further processing, as it would be a different entity processing, emphasised the importance of ensuring third parties are transparent with data subjects and that there is a lawful basis for any change of data controller.

The government judges that there is sufficient support for clarifying on the distinctions between new processing and further processing.

Clarifying further processing when the original legal basis is consent (question 1.3.4):

The government asked whether there was a need for clarification on further processing where the original legal basis is consent. The majority of respondents agreed that clarification would be beneficial and would support transparency. Many supportive respondents that the concept of consent must be respected in relation to re-use.

The government plans to clarify that further processing cannot take place when the original legal basis is consent, other than in very limited circumstances.

1.4 Legitimate interests

Data controllers are currently required to complete a 3 part test when relying on the legitimate interests lawful ground under Article 6(1)(f) of the UK GDPR.

They must:

1. identify a legitimate interest;
2. demonstrate the processing is necessary for the intended purpose and cannot be achieved through less intrusive means; and
3. weigh up whether their interests in processing personal data outweigh the rights and data subjects.

The third part of the legitimate interests assessment is sometimes known as the balancing test. The government proposed that the balancing test for the legitimate interest assessment is discretionary to help demonstrate compliance.

Prior to consulting, the government was aware that some organisations were concerned about the time and resource required to carry out legitimate interests assessments. Others perceived using the legitimate interests lawful ground as more complicated and risky than other grounds. They were concerned that they might be required to demonstrate to the ICO, upon request, that they had carried out themselves being investigated by the ICO, which could lead to potential enforcement action for breaching rules. Organisations tended to seek individuals' consent to reduce the risk of being in breach of the rules, and to avoid potential reliance on consent. Consent fatigue for some customers and service users.

Exemptions for legitimate interest balancing test (questions 1.4.1, 1.4.2, 1.4.3, 1.4.4):

To address these issues, the government proposed to create a limited, exhaustive list of legitimate interests for which organisations could use personal data without applying the balancing test. The government also proposed that certain activities could be suggested several processing activities for consideration as part of such a list.

Some were included because of the public interest benefits of the activity, such as:

- processing that is necessary for the purposes of crime prevention and safeguarding
- enabling non-public bodies to deliver statutory public communications and public health and safety messages

Others involved non-intrusive uses of personal data for commercial purposes, for example:

- processing of customer data for the purposes of installing security updates on a product
- processing personal data for internal research and development purposes
- processing personal data for business innovation purposes that are aimed at improving services for customers

The government's proposals in this area were that some organisations were concerned about the time and resource required to carry out legitimate interests assessments. Others perceived using the legitimate interests lawful ground as more complicated and risky than other grounds. They were concerned that they might be required to demonstrate to the ICO, upon request, that they had carried out themselves being investigated by the ICO, which could lead to potential enforcement action for breaching rules. Organisations tended to seek individuals' consent to reduce the risk of being in breach of the rules, and to avoid potential reliance on consent. Consent fatigue for some customers and service users.

Exemptions for legitimate interest balancing test (questions 1.4.1, 1.4.2, 1.4.3, 1.4.4):

To address these issues, the government proposed to create a limited, exhaustive list of legitimate interests for which organisations could use personal data without applying the balancing test. The government also proposed that certain activities could be suggested several processing activities for consideration as part of such a list.

Some were included because of the public interest benefits of the activity, such as:

- processing that is necessary for the purposes of crime prevention and safeguarding
- enabling non-public bodies to deliver statutory public communications and public health and safety messages

Others involved non-intrusive uses of personal data for commercial purposes, for example:

- processing of customer data for the purposes of installing security updates on a product
- processing personal data for internal research and development purposes
- processing personal data for business innovation purposes that are aimed at improving services for customers

The government's proposals in this area were that some organisations were concerned about the time and resource required to carry out legitimate interests assessments. Others perceived using the legitimate interests lawful ground as more complicated and risky than other grounds. They were concerned that they might be required to demonstrate to the ICO, upon request, that they had carried out themselves being investigated by the ICO, which could lead to potential enforcement action for breaching rules. Organisations tended to seek individuals' consent to reduce the risk of being in breach of the rules, and to avoid potential reliance on consent. Consent fatigue for some customers and service users.

These responses were from respondents that creating a limited exhaustive list would give organisations greater confidence in their personal data. Of the respondents that agreed, some suggested that further everyday business activities, such as human resources, should be included in the exhaustive list. Similarly, a majority of proponents of such reforms nevertheless highlighted the importance of including such as a precise definition of relevant processing activities, in order to avoid misuse of the exemption. Some respondents also suggested that there should be consideration to protect the rights of individuals, and social concern about the impact of removing the balancing test on levels of public trust.

The vast majority of respondents agreed that the balancing test should be maintained for children's data, with very minimal disagreement.

In response to the consultation question, the government seeks to pursue the proposal in relation to all the relevant processing activities, including defined processing activities. This is likely to include processing activities which are undertaken by data controllers to pursue legitimate interests that are not listed in the exhaustive list, but which are important reasons of public interest. The government proposes to create a power to update the list of activities in case other processing activities are identified that should be added to the list. Any changes would be subject to parliamentary scrutiny.

The government recognises how important it is to ensure this approach continues to be proportionate and fair. The list of activities in the legitimate interests recognised by government will consider if any additional safeguards are needed for certain cases. This may not be necessary where the inclusion of an activity has been added to the list of legitimate interests following a public interest balancing test that has already taken or being other steps to protect the welfare of children. In addition, data controllers would still need to demonstrate that processing for one of the listed activities complied with the other UK GDPR requirements, including the principles in Article 5 of the UK GDPR. Where the processing involved special category data, the controller would also need to meet the requirements for lawfulness and safeguards in Article 9 of the UK GDPR and Schedule 1 to the DPA 2018.

For accompanying activities that do not feature on the list, data controllers will continue to be required to undertake the balancing test.

1.5 AI and machine learning

As set out in the consultation document, when used responsibly, data-driven artificial intelligence (AI) technologies have the potential to transform the economy. However, the development of AI and machine learning applications is contingent on data, and places demands on the collection, curation and use. The government's consultation focused specifically on the interplay of AI technologies with the UK's data protection regime.

Following the publication of the National AI Strategy in September 2021, the government's ambition is for the UK to be the leading AI economy. The strategy set out how the government plans to build on the UK's leadership in AI, across its research, development and commercialisation, and to ensure the UK's AI ecosystem is trusted.

The consultation proposed some reforms to help organisations to build or deploy AI systems responsibly, and to innovate with care, while ensuring rules are managed and individuals can trust that their data rights are respected.

Fairness in AI (current Questions 1.5.1.1.5.1.1.5.1.6.1.5.1.6)

Whilst AI governance is a live debate, the government expects AI systems (and their use) to be fair. Fairness' is a highly context-specific concept, and consists of fairness which is a variety of legislative frameworks, navigating fairness in the context of AI is complex. Fairness in AI is a live debate, and the government's approach to AI and machine learning and AI, and there is a position of how data protection law interacts with fairness in the context of AI.

The government sought views on whether the current legal obligations regarding fairness are clear (both in terms of developing AI-driven technologies, and within the existing data protection regime). The government also sought views on what legislative or non-legislative mechanisms could be the assessment of controller compliance with fairness (especially in outcomes).

There were mixed views on whether the current obligations are sufficiently clear with regards to fairness when developing or deploying AI system. Similarly, views were mixed regarding the overall clarity of fairness requirements the existing data protection regime, and how it interacts with other legislative regimes. Many of the respondents raised a degree of confusion around how fairness obligations under the data protection regime interact with other legislative regimes, such as those on discrimination. Others considered the development of a 'substantive concept of fairness' in relation to AI. Many of the respondents also highlighted that many respondents agreed that the development of a substantive concept of substantive fairness within the data protection regime would pose risks. There was some disagreement on the extent to which the data protection regime (and data protection law) is fit-for-purpose and is best placed to effectively cover all possible AI use cases across the economy on the basis that there is personal data involved.

The consultation also asked a range of open questions about AI and fairness.

Respondents highlighted the importance of measures and safeguards which exist in the wider realm of fairness, though are traditionally outside of the data protection law. Such measures include:

- guidance to support AI practitioners and developers to use current fairness and bias mitigation tools in the AI development process
- periodical evaluations of the individuals and entities involved in development
- participation of affected stakeholder groups in the wider development process
- conducting and publishing Algorithmic Impact Assessments

There was support for regulators playing a role in substantive assessments of fairness, including the ICO. Many noted the ICO's existing work on fairness, including the Financial Conduct Authority (FCA), although there was not a definitive consensus. Respondents noted that there is need for regulatory coordination between different regulators, for fairness (and).

There were no consensus on whether data protection legislation would be the right place to address broader AI governance fairness issues. Responses did indicate that:

- Issues of fairness in data protection need to be considered as part of a holistic approach to AI governance
- Issues of fairness also arise from the use of personal data which are not in scope of data protection legislation
- the role of the ICO should be included in the wider regulatory landscape

The government will consider the role that fairness should play in wider AI governance as part of the white paper on AI governance, but does not currently plan to legislate on this.

Building trustworthy AI systems (questions 1.5.5, 1.5.6, 1.5.7, 1.5.8, 1.5.9)

In the consultation document, the government asked a range of open questions about the potential mechanisms that could be introduced to ensure that AI systems using personal data are fit-for-purpose and that the processing of developing AI systems, and whether organisations have difficulty navigating trade-off or lack of clarity in the interplay between AI and data protection. The government also sought views on the potential of some but there were no clear themes. Some respondents stated that they would benefit from further clarity on the types of organisations to which provisions or requirements would apply, and how they would apply, while others suggested that the existing guidance on lawful grounds is sufficient.

The use of AI-powered automated decision-making is likely to increase substantially in the coming years. Currently, Article 22 of the UK GDPR sets out the rules on automated and profiling by data controllers. The government recognises that organisations working in AI tools need the space to experiment without causing harm. The consultation proposed to clarify the lawful grounds for processing personal data more freely for the purposes of testing and training AI. The majority of respondents disagreed that there is a need, at present, to change the current requirements on the lawful grounds for processing personal data for the purposes of testing and training provisions already enable organisations to experiment.

Bias mitigation in AI (questions 1.5.10, 1.5.11, 1.5.12)

Another key aspect of AI trustworthy AI systems is ensuring organisations are aware of potential biases in the datasets. As set out in the consultation document, bias monitoring and correction can involve the use of personal data.

The government sought views on whether processing such data for the purpose of bias monitoring, detection and correction raises any data protection concerns or challenges, can rely on its vital and protecting, without applying a balancing test. The government also sought views on whether further lawful rights (related, and whether paragraph 9 of Schedule 1 to the DPA 2018 is, or could be, drafted broadly enough to allow organisations to undertake such processing of sensitive data for the purposes of bias monitoring and correction, subject to appropriate safeguards.

The majority of respondents agreed that there should be additional legal clarity on how sensitive data can be lawfully processed in relation to bias monitoring and correction in AI systems. Respondents noted that this would help to ensure there is clarity and confidence for the processing of sensitive data to bias monitoring and correction, and that it would be beneficial to include this in the DPA 2018 as a new condition in paragraph 9 of Schedule 1. Many respondents highlighted concerns around the proportionality of such a provision, and that safeguards were in place to prevent and the government recognises these concerns.

The government plans to introduce a new condition to Schedule 1 of the DPA 2018 to enable the processing of sensitive personal data for the purpose of ensuring and correcting bias in AI systems. The new condition will be subject to appropriate safeguards, including a requirement for controllers to demonstrate why and processing measures when processing for this purpose.

The majority of respondents disagreed with the proposal to include bias monitoring in lot of legitimate interests, although there was some support for the proposal. Respondents noted that bias monitoring is a vital activity, and it is appropriate proportionate to the potential harm of bias within a particular system.

As indicated in Question 1.4 (legitimate interests)(Q1.4), the government intends to remove the balancing test only in relation to an initially limited number of carefully defined activities. The list of activities in Annex 1 of the consultation document (Q1.4) contains as part of the list. This means that organisations processing data for these purposes could still rely on the legitimate interests lawful ground where appropriate, but would need to undertake the balancing test in the normal way.

Rights in relation to automated decision-making and profiling (Article 22) (questions 1.5.13, 1.5.14, 1.5.15, 1.5.16)

As outlined in the consultation document, the Enhanced fairness of AI systems hinges on specific design features, but also on effective safeguards where they neither. The government sought views on the proposed approach to reform Article 22 of the UK GDPR contains provisions on automated decision-making profiling. Not all AI systems trigger the application of Article 22 - only decision-making processes that are solely automated, and which have a legal or similarly significant effect on the data subject, which is not 'yes' and not in Article 22(1) UK GDPR. The government sought views on clarifying the limits and scope of what constitutes a 'decision made solely by automated means' and what is a 'similarly significant effect' in the context of whether Article 22 is sufficiently future-proofed, practical, and proportionate.

Consultation responses demonstrated that the current operation and efficacy of Article 22 is subject to uncertainty. Respondents noted confusion with the term 'solely' and the ambiguity over the requirements for human involvement needed for a decision not to be 'solely automated'. Many respondents noted that Article 22 is unclear and can be highly context-specific whether a decision causes a significant effect (falling within the scope of Article 22). Many respondents noted that Article 22 is not fit-for-purpose in the modern digital economy, such as traditional human rights concerns with profiling and scope, with respondents providing mixed views on whether Article 22 is fit-for-purpose, and whether it is in its current form, it is capable of being interpreted in meaningful safeguards.

The vast majority of respondents supported the proposal to remove Article 22, with respondents noting that the right to human review of an automated decision was a key safeguard, and that its removal would be a significant change that could risk damage the reputation of the United Kingdom as a trustworthy jurisdiction for carrying out automated decision-making. The government recognises the importance of appropriate safeguards, and will not pursue this proposal.

The government is considering how to amend Article 22 to clarify the circumstances in which it can be applied to AI systems, and how it could be amended to ensure that the Europe approach to governing AI-powered automated decision-making that will be in the future UK-EU Adequacy assessment. The government will keep Article 22 as it right to specific safeguards, rather than as a general prohibition on solely automated decision-making. Reforms will enable the benefits of AI-powered automated decision-making, providing scope for innovation with appropriate safeguards in place.

Public trust in the use of data-driven AI systems (questions 1.5.18, 1.5.19, 1.5.20)

Public trust in data-driven AI systems is essential for the successful adoption of AI. Good data protection tools, processes and definitions to address profiling issues and their impact on specific groups, what, if any, legislative changes the government could make to further clarify the application of the UK GDPR in the context of AI, and what is sufficient, but crisper guidance would be beneficial, particularly if developed through collaboration between regulators. The government will consider further the interplay between data protection and competition law in digital markets, including the role of data protection legislation within that, through the wider paper on AI governance.

1.6 Data minimisation and anonymisation

UK data protection legislation requires that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed, a commonly known as the data minimisation principle. Data minimisation techniques, such as pseudonymisation, can be applied to personal data sets to safeguard them. Under the UK GDPR, pseudonymised personal data is personal data. The difference between pseudonymisation and anonymisation is important as pseudonymised data falls within the data protection legislation, whereas anonymous data does not.

Clarifying data regarded as anonymous (questions 1.6.1, 1.6.2, 1.6.3)

The government sought views on whether the current data protection law defined as anonymous and therefore outside the scope of data protection legislation. The consultation proposed legislating to confirm that the test for whether anonymous data is identified is relative to the means available to the controller or to identify the data.

The majority of respondents agreed that greater clarity in legislation would be beneficial, although many were cautious about defining pseudonymisation in a way that is dynamically high standard to achieve would be create the test of the. Some respondents suggested that the test should be based on a creative use, and a limited number of respondents disagreed with the proposal.

The government therefore intends to clarify in legislation, when a living individual is identifiable, that it is a relative test dependent on the means of the data controller or is a relative one, and that the test should be based on the wording set out in the explanatory report to the Council of Europe's Convention 108+.

This could be where a living individual is identifiable by the controller or processor by "reasonable means". Taking into account, among other things, the technology available at the time of processing and technological developments. If the means are held by the controller or processor known, or ought reasonably to know, that passing the data to another data controller or processor is likely to result in re-identification. Taking into account the means available to the recipient.

By confirming the test for anonymous data as relative, and incorporating the wording from the explanatory report to Convention 108+ which focuses on the means that are reasonably likely to be used to identify data, the government intends to avoid setting an impossibly high standard for anonymisation.

Privacy enhancing technology (questions 1.6.4)

The consultation asked an open question about whether there is more that the government could do to support the development of PETs. Section 128 of the DEA contained mandatory PETs research and development was highlighted, as well as a commitment to work with the ICO to ensure the UK's data protection regime is world PETs and the Centre for Data Ethics and Innovation's (CDEI) recent review into PETs. The vast majority of respondents agreed that the government should be driving the uptake, maybe the potential adoption of PETs, rather than just their use.

The government also noted that some respondents advised caution about overcoming or what PETs can achieve. They suggested PETs could be promoted as a means of data minimisation, and that organisations should not view PETs as a substitute for wider organisational measures that can help reduce privacy risks. The government will continue to engage with the ICO to ensure the adoption of PETs is encouraged as part of organisations' approach to privacy management.

The government is also keen to explore opportunities with its international partners to promote the development and adoption of PETs, building on the 'Joint Statement' announced plans to work with the United States to collaborate on research and develop pilot projects focused on advancing privacy enhancing technologies (PETs).

1.7 Innovative data sharing solutions

Responsible data sharing solutions can help drive growth and boost innovation, and the government aims to encourage new and innovative ways that confidential (personal or business) data can be shared securely and lawfully. Intermediaries, or third intermediaries can help connect confidential data between those holding it and those using it, in a responsible and efficient manner.

This inequity is nascent and the government sought views on its role in enabling the activity of data intermediaries. A range of open questions were asked about what lawful mechanisms could be used to ensure that data intermediaries are fair and transparent, trusted, and creating accountability schemes to ensure the responsible management of data.

The government has a long-standing commitment to legislate to enable the development of Smart Data Schemes. We are working to ensure that such legislation does not preclude the possibility for a range of data intermediaries to offer services on these schemes, and to ensure that the UK's data protection regime does not pose a potential participation to be appropriately managed through regulation.

The government will work to ensure any regulations establishing and setting out the framework for future Smart Data schemes are appropriately scoped to maximise the benefits of data intermediaries while mitigating any risks they pose. We will also ensure that the data protection regime does not pose a barrier to the use of data intermediaries, including for example by enabling individuals to exercise their data rights in complex, high-volume data sharing that could be enabled by intermediaries operating at scale. The government will also consider the role of data protection in relation to intermediaries, setting rights and obligations, and testing promoting approaches to data protection compliance.

Lawful grounds regarding data intermediaries (question 1.7.2)

The consultation asked various open questions on whether lawful grounds, other than consent, could be used by data intermediaries. The vast majority of respondents agreed that other lawful grounds might be applicable otherwise legitimate interest as an alternative lawful ground. Respondents who disagreed believed that consent should be the only lawful ground. The government will keep this under consideration in relation to the question but will factor respondents' comments into any potential future policy making in this area.

1.8 Further questions

At the end of the chapter, the government asked for views on whether any of the proposals in this chapter would, if taken forward, give rise to any equality law specific concerns related to the impact on protected groups and those in their with protected characteristics.

The consultation posed some open-ended questions at the end of this chapter for respondents to provide any other comments on the proposed reforms. The most significant issues raised by respondents in relation to the further questions posed at the end of this chapter.

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

2.1 Summary

In chapter 2 of the consultation, the government considered how to provide a high standard, flexible data protection regime, whilst ensuring that businesses can benefit from an agile regulatory approach, as described in the government's Plan for Digital Regulation.

The government highlighted the opportunity to develop a regime that incentivises organisations to adopt practices that go beyond the minimum legal requirements, and to better outcomes for both businesses and individuals. The government's proposed reforms aim to deliver greater flexibility and more proportionate and targeted accountability measures, while ensuring that the UK's data protection law is not creating a disproportionate regulatory burden with limited value for individuals.

2.2 Reform of the accountability framework

The government views the principle of accountability as fundamental, but also recognises that the current prescriptive approach to accountability means that they are complying with the data protection regulation can put a disproportionate burden on organisations. The government's proposed reforms to introduce a more flexible accountability framework, underpinned by "privacy management programmes". The chosen organisation would be required to take to implement an effective programme around reflect the volume and sensitivity of the personal data processed.

The privacy management programme approach would be based on a number of elements of the core of accountability, such as:

- leadership and oversight
- data protection risk
- policies and processes
- transparency
- monitoring and assessment of staff
- monitoring, evaluation and improvement

To support the implementation of privacy management programmes, the government also proposed removing the existing requirements:

(i) designate a data protection officer under Articles 37 to 39;
(ii) undertake data protection impact assessments under Article 35; and
(iii) maintain a record of processing activities under Article 30.

In their place, the government proposed complementary measures under the privacy management programme, such as:

(i) appointing a suitable senior individual to be responsible for the programme;
(ii) undertaking a risk assessment or risk assessment tools which help assess, identify and mitigate risks; and
(iii) a more flexible record-keeping requirement.

Reform of the accountability framework (question 2.2.1)

The majority of respondents disagreed that the proposed framework should feature fewer prescriptive requirements and be more risk-based, as they respondents consider the current requirements to be flexible and scalable. Many respondents noted that most of respondents agreed, with those who supported a need to reform the accountability framework arguing that a more flexible and risk-based approach will lead to better outcomes for individuals, and that the Risk-based approach to data complying and demonstrating compliance.

However, when looking at responses from organisations only, the majority of respondents disagreed that the current UK GDPR is too prescriptive. Respondents and Organisations responded that adopting a more flexible approach to accountability would provide flexibility to allow organisations to focus their resources more effectively.

Introduction of new privacy management programmes (questions 2.2.2, 2.2.3)

There were mixed views regarding whether organisations will benefit from being required to develop and implement a privacy management programme. Many respondents noted that the proposed reforms would be beneficial for organisations with privacy management programmes. Some of those who opposed the proposal or were unsure noted that organisations would need to implement new processes and have to comply and generally incorporate customer's data subjects, and that further regulatory changes would be costly to implement. However, those who were in favour of the proposal noted that it would be beneficial to organisations, as it would prevent crises of risk and be a pragmatic approach to be taken by organisations, and that privacy management programmes would help establish a one-size-fits-all approach, which would be particularly helpful for small and medium-sized enterprises (SMEs).

The government plans to proceed with the requirement for organisations to implement privacy management programmes, with the significant proposed to take into account concerns raised during the consultation process. In particular, the government recognises the concerns of respondents that the current UK GDPR has organisations have invested to establish policies and processes in order to comply with the UK GDPR, and that any further regulatory changes would lead to further costs.

The government also proposed to remove the requirement for organisations to implement a mandatory "accountability" framework, and instead, proposed a more flexible approach to accountability. This means organisations that are currently compliant with the UK GDPR would not need to make significant changes to their existing practices with the new requirements, unless they wanted to take the advantage of the additional flexibility that the new legislation will provide. Furthermore, the government believes that the new approach will allow for a shift in focus from ticking boxes to achieving outcomes for individuals, as organisations will have the flexibility to prioritise activities to meet the outcomes of the new regime, rather than following a tick-box process.

The principle of accountability is key for privacy management programmes, and organisations will be required to take into account the ICO's accountability framework under the new regime. A move to a framework based on privacy management programmes will enable organisations to take a more proportionate approach to data protection compliance, and will allow the ICO to focus on more prescriptive regulatory burdens placed by smaller organisations, while enabling more organisations to focus on the outcomes required to help demonstrate compliance to regulatory bodies.

The government's consultation recognises that organisations will be required to comply with standards. However, under the revised regime, organisations will have to implement a privacy management programme that is proportionate to the volume and sensitivity of personal data they handle. Therefore, organisations that process highly sensitive data (i.e. special category data) or large volumes of high-risk data will need to implement a more robust privacy management programme. The government believes that privacy management programmes will place greater emphasis on the principles of the core of accountability such as organisational governance and oversight, data protection risk assessments, policies and processes, and continuous monitoring, evaluation and improvement of data protection management within an organisation.

To align with the existing expectations, the privacy management programme requirement will be mandatory for public authorities as under the current regime, covering maximum fines of the greater of £10 m or 2% of annual worldwide turnover.

Removal of data protection officers (questions 2.2.4, 2.2.5, 2.2.6, 2.2.7)

The UK GDPR requires certain organisations to appoint a data protection officer (DPO) or designate a data protection officer. Respondents to mainly shared concerns that removal of the data protection officer requirement would result in a loss of data protection expertise and would lead to a lack of independence, and would result in a loss of resources to data subjects. Whilst many individuals felt their organisations would not maintain a similar role if it was no longer mandatory, most organisations said that they would. Many organisations noted that they would retain a data protection officer, and designate a data protection officer mentioned that they would be beneficial for smaller organisations, and that it would be beneficial for services highly sensitive personal data. A small proportion of respondents have suggested that it is difficult to find a suitable who is truly independent.

The new requirement to appoint a senior responsible individual will shift the emphasis from a prescriptive requirement to a more flexible approach to embedding a culture of data protection. For that reason, the government plans to proceed with removing the requirement to designate a data protection officer. Most of the barriers a to the appointment of a DPO will be removed, and organisations will appoint a senior individual to oversee as part of the privacy management programme.

The designated senior individual's role will include:

- responsibility or delegating responsibility for the DCO and data subjects
- ensuring appropriate oversight and support is in place for the programme and assembling appropriate personnel
- providing tailored training to ensure staff understand the organisation's policies and procedures, and the wider data protection law

The government is considering the role of the senior responsible individual, and whether it comes to the designation of the data protection officer. The primary consideration is whether the role of the senior responsible individual is sufficiently independent to effectively monitor the organisation's data protection compliance, and oversight from the senior accountable individual. For example, some organisations that have implemented the senior responsible individual role have found it beneficial to have data protection officers above they consider that it the best way to monitor and improve compliance.

Removal of data protection impact assessments (questions 2.2.8, 2.2.9)

The majority of respondents agreed that data protection impact assessments requirements are helpful in identifying and mitigating risk, and disagreed with the proposal to remove the requirement to undertake data protection impact assessments. However, many respondents noted that they would still undertake data protection impact assessments, which would place them to be replaced by a less prescriptive requirement. Many organisations noted that they would be in favour of more prescriptive digitalisation of other risk assessments that achieve the same outcome. Some respondents noted that the current requirements are burdensome and time-consuming, and that a less onerous approach would be beneficial, and that some of the requirements under the data protection impact assessment requirement.

Under the new privacy management programme, organisations will be required to identify and manage risks, but they will be granted greater flexibility as to how to meet the requirements, and how to demonstrate compliance. The new requirement to undertake data protection impact assessments has proven to be burdensome for UK SMEs, and is required to ensure there are risk-assessment tools in place for the identification, assessment, management, monitoring and minimisation of data protection risks. In recent, the government has proposed to remove the requirement to undertake data protection risk assessments. The government understands from the consultation responses that organisations will need to undertake data protection risk assessments to comply with the privacy management programme and to continue to be accountable. However, the government believes that a less prescriptive approach to data protection risk assessments will allow organisations to focus on the outcomes required to help demonstrate compliance to regulatory bodies.

Under the new privacy management programme, organisations will be required to identify and manage risks, but they will be granted greater flexibility as to how to meet the requirements, and how to demonstrate compliance. The new requirement to undertake data protection impact assessments has proven to be burdensome for UK SMEs, and is required to ensure there are risk-assessment tools in place for the identification, assessment, management, monitoring and minimisation of data protection risks. In recent, the government has proposed to remove the requirement to undertake data protection risk assessments. The government understands from the consultation responses that organisations will need to undertake data protection risk assessments to comply with the privacy management programme and to continue to be accountable. However, the government believes that a less prescriptive approach to data protection risk assessments will allow organisations to focus on the outcomes required to help demonstrate compliance to regulatory bodies.

Reform of data protection impact assessment (questions 2.2.10, 2.2.11)

The majority of respondents agreed that data protection impact assessments requirements are helpful in identifying and mitigating risk, and disagreed with the proposal to remove the requirement to undertake data protection impact assessments. However, many respondents noted that they would still undertake data protection impact assessments, which would place them to be replaced by a less prescriptive requirement. Many organisations noted that they would be in favour of more prescriptive digitalisation of other risk assessments that achieve the same outcome. Some respondents noted that the current requirements are burdensome and time-consuming, and that a less onerous approach would be beneficial, and that some of the requirements under the data protection impact assessment requirement.

Under the new privacy management programme, organisations will be required to identify and manage risks, but they will be granted greater flexibility as to how to meet the requirements, and how to demonstrate compliance. The new requirement to undertake data protection impact assessments has proven to be burdensome for UK SMEs, and is required to ensure there are risk-assessment tools in place for the identification, assessment, management, monitoring and minimisation of data protection risks. In recent, the government has proposed to remove the requirement to undertake data protection risk assessments. The government understands from the consultation responses that organisations will need to undertake data protection risk assessments to comply with the privacy management programme and to continue to be accountable. However, the government believes that a less prescriptive approach to data protection risk assessments will allow organisations to focus on the outcomes required to help demonstrate compliance to regulatory bodies.

Removal of the record of processing activities requirement (questions 2.3.01, 2.3.02)

The government also sought views on whether the requirement to maintain a record of processing activities should be removed, and whether organisations should use flexible record keeping requirement under the privacy management programme.

The majority of respondents disagreed with the proposal to remove this requirement. Many respondents felt that the existing requirement is not burdensome and should be retained to ensure that organisations are accountable for personal information they hold. However, a minor number of respondents felt that the current requirement is burdensome. Some of these respondents noted that the record keeping requirements in the legislation, and would therefore welcome greater flexibility to take a more tailored approach to record keeping.

Respondents were also asked whether or not elements of record keeping requirements are duplicative of Articles 30 and 35 without any particular benefit. Around half of respondents agreed that some of the record keeping requirements do duplicate the fundamental building blocks which their keeps them to comply with the requirements under Articles 30 and 35 to inform individuals about how their data is going to be used and how it is being used. Around half felt that the record keeping requirement in GDPR was duplication without any particular benefit.

Organisations will need to have personal data inventories as part of their privacy management programme which describe what and where personal data is held, why it is held, and how it is used. This is a key element of the accountability principle and was prescribed by the requirements set out in Article 30. For that reason, the government proposed that the record keeping requirement be included in the privacy protocol. Privacy management programmes will still require organisations to document the purposes of processing, but in a way which is more tailored to the organisation.

Overall, the new regime will continue to require organisations to maintain the same high standard of data protection as under the current regime. This will ensure that it still reflects the volume and sensitivity of the personal data they handle, and the type of data processing they carry out. The government believes that providing a new flexible record keeping requirement in the form of a privacy management programme, rather than even a prescriptive list, will also lead to greater transparency practices. This is because organisations will need to focus more on the data they actually process and how they can demonstrate effective privacy management programme, and how they effectively communicate their programmes to relevant data subjects.

Prior consultation requirements (question 2.3.03)

The government wants to further encourage a more proactive, open and collaborative approach between organisations and the ICO, and to ensure that organisations identify and mitigate risks. Under Article 36 (2) of GDPR, if organisations identify a data processing activity which poses high risks which cannot be mitigated, they must inform the ICO. The government is aware that compliance with Article 36 is low.

The consultation put forward a proposal to remove the mandatory requirement for organisations to consult the ICO prior to processing personal data where they have undertaken a data protection impact assessment and the response is outstanding for more than two months. The government believes that this will encourage organisations to take a more proactive approach to data protection by ensuring that they have the time they need to deal with any issues discovered as a result of undertaking a data protection impact assessment, and to resolve the problem.

Around half of respondents agreed with the proposal and around a third disagreed. Concerns were raised that the process may be of limited use to small and medium sized organisations, because they may not have the resources to undertake a data protection impact assessment in the first place, and that organisations without documented prior engagement with the ICO might not benefit. Moreover, the current framework already provides a strong incentive for organisations to consult with the ICO prior to processing action taken, if non-obtaining the ICO's verify compliance under Article 32(3) of GDPR. As such, the government will not be pursuing this proposal.

Breach reporting requirements (question 2.3.03)

Breach reporting requirements are set under Article 33 of the UK GDPR. These requirements state that a breach must be reported to the ICO if it is likely to result in a risk to the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons'. In practice this has led to the reporting of some relatively minor breaches, such as the loss of a password protected USB stick. The government therefore sought views on the impact of changing the threshold for reporting a personal data breach, so that only breaches which posed 'material risks' to the rights and freedoms of individuals.

Responses to the consultation were mixed. Between, those that thought it might reduce disproportionate burdens on businesses, those that thought it would make no difference, and those who felt it would increase burdens. Some felt it would confuse [illegible] and those who thought it could reduce protections for individuals, with regard to the latter, some organisations pointed out that the true severity of a breach is not always known at the time of the breach, and that it may be the case that breaches seen like a minor breach to one organisation might be a become a more serious breach if the same mistake was repeated across a wider sector.

Some respondents, including the ICO, felt that this would impact a negative change in this area could have, if it led to a reduction of valuable intelligence data for the ICO to monitor and regulate breaches. Around half of respondents also thought that additional guidance from the ICO on when to report a breach would be more helpful in reducing burdens on them than legislative changes.

The government has decided not to pursue this proposal, because of a legislative change, but will continue to work with the ICO to complete the Beyond Compliance project for organisations on breach reporting.

The consultation proposed alternative clarations reforms if the government chose not to pursue the implementation of the privacy management programme. As the government has decided to pursue the implementation of the proposed requirement privacy management programmes, these will not be pursued.

2.3 Subject access requests

The right of access is one of the key rights of the data protection framework, and subject access requests are an important part of this. They allow for data subjects to find out what data is held about them, learn more about how it is being used, and what it is being shared with.

While subject access requests are a critical mechanism to empower data subjects to understand and control their data, dealing with requests can be time consuming and resource intensive for organisations.

Resource impact of subject access requests (question 2.3.1)

The government asked an open question on the extent to which organisations found subject access requests burdensome. Responses to this question were received from a variety of small and large organisations, including SP organisers, local councils, telecoms providers, and property, financial and legal services. Round dealing with subject access requests was felt to be time consuming and resource intensive by charity and non-profit, legal, financial, public and health/psychiatrist the level of resourcing required to respond to subject access requests could be very high. Responses to the ICO's Call for Evidence noted that subject access requests can be used as a means of circumventing strict disclosure protocols, to pursue other grievances, or to gain information for use in other disputes. The ICO noted that changes to the subject access requests regime, emphasised the importance of data subjects having access to information held about them.

'Manifestly unfounded' threshold for subject access requests (question 2.3.2)

The government outlined ones or whether the 'manifestly unfounded' threshold for refusing to respond to, or charge a reasonable fee for a subject access request was too low. The ICO's Call for Evidence noted that the ICO's Call for Evidence noted that the threshold is often perceived as too vague to encompass requests which are clearly unreasonable in nature and should be allowed to be refused, such as requests from individuals who are clearly using to harm their subject access requests, should their former employer.

Consultation respondents also noted that some claims management companies are using subject access requests to pursue claims against their former employers. Information relating to their clients has been omitted in their responses. Other noted that further guidance on the time limit for responding to a subject access request would be helpful. The ICO noted that it is currently developing a new guidance and tools and processes to handle subject access requests to alleviate the time and effort in responding to requests.

Alignment with the Freedom of Information regime (introducing a cost limit and amending the threshold) (question 2.3.3)

The government also sought views on ways to align the subject access request regime with the Freedom of Information request regime, and whether to:

(i) introduce a cost ceiling, and

(ii) amend the threshold from 'vexatious' to 'excessive' to alleviate organisations' concerns when responding to subject access requests.

There were mixed views on these proposals. Organisations in favour of a cost limit argued that it would be particularly beneficial to SPRU and make complying with subject access requests more manageable. Those who were not in favour of a cost limit argued that it would be difficult to set the cost limit at a level that would not hamper the public's understanding of how their personal data is being used.

The government recognises that the rights of all data subjects must be protected, including vulnerable people. Information provision, and the right of access, remains the key right.

Taking into account views expressed as part of this question, as well as the question regarding the 'manifestly unfounded' threshold above, the government plans to proceed with changing the current threshold for refusing or charging a reasonable fee for a subject access request from 'manifestly unfounded' to 'manifestly excessive', which will bring it in line with the Freedom of Information regime. The government does not intend to introduce a cost ceiling for subject access requests.

Introducing a vexatious fee (question 2.3.4)

The government also asked whether there was a case for introducing a small nominal fee for processing subject access requests, as is the case under the Freedom of Information Protection Act 2000. The majority of respondents disagreed with this proposal. Respondents felt it could disadvantage more vulnerable people in society, although other respondents felt it may discourage vexatious and repetitive requests.

The government does not intend to introduce a nominal fee for processing subject access requests. The government is concerned that this could disproportionately discourage organisations to implement appropriate processes and procedures to respond well to subject access requests.

Finally, the government is considering how to address specific sectoral needs as raised in the consultation response (e.g. healthcare) as well as those of small and medium sized businesses.

2.4 Privacy and electronic communications

Whilst the majority of the consultation focused on possible changes to the UK GDPR and DPA 2018, Annex B of the DCMS consultation document also proposed changes to the Privacy and Electronic Communications Regulations 2003 (PECR). PECR supplements the UK GDPR with specific rules relating to confidentiality of terminal equipment (e.g. cookies), unsolicited marketing communications (including by telephone, automatic calls), and communications security (e.g. network traffic and location data). PECR's rules protect companies as well as individuals.

Cookies (questions 2.4.1, 2.4.2, 2.4.3, 2.4.4, 2.4.5, 2.4.6, 2.4.7, 2.4.8)

Under the current regulation, cookies (and similar technologies such as tracking pixels) are not allowed to be placed on a device without the consent of the user.

There are currently only two limited exceptions from gaining consent. These are:

(i) if a cookie is used for the purpose of providing an online service at someone's request (e.g. to remember what's in their online basket, or to ensure security in online banking);

(ii) where needed to transmit a communication over a communications network.

Consent is usually sought through a pop-up notice or banner which appears when a person visits a website. Some respondents suggested that their ability to collect potentially useful information, such as how many people are visiting their websites and which pages people are looking at, is being affected by the requirement to obtain consent. Individuals also find the number of cookie pop-ups a source of annoyance, and routinely accept the terms without reading them.

The government also sought views on whether there were any other circumstances where cookies (and similar technologies such as tracking pixels) could be permitted to be placed on a person's device without their explicit consent. This could include, for example, where it is for the purpose of statistical or analytical purposes or for the purpose of detecting faults on an organisation's website.

The majority of respondents agreed with the proposal that organisations should be able to use cookies and similar technologies without consent for a wider range of non-intrusive purposes, although there was some disagreement. The majority of respondents felt that cookies should be allowed for purposes of internet traffic to a website and improve its offering to users should for instance.

The government also sought views on whether prior consent should be removed for all types of cookies, particularly more intrusive varieties which collect personal data for purposes such as behavioural advertising and online behavioural tracking. Many respondents argued that web users should be given clearer information about these types of cookies so that they could exercise their right to reject them where appropriate.

There was also support for websites respecting individuals' preferences set through browser settings to reject cookies being placed on their devices. Some respondents felt that it would increase user experience and benefit trust in those using services, but this would need to be balanced against the fact that many users access different platforms and services would have the technological capability to provide signals consistent technology.

Following consideration of responses, the government intends to legislate to remove the requirement for consent for all types of cookies. This will ensure that the use of the government will permit cookies (and similar technologies) to be placed on a user's device without explicit consent, for a small number of other non-intrusive purposes, such as those for the purpose of statistical or analytical purposes, including cookies opt-in smartphones, tablets, smart TVs or other connected devices.

In the future, the government intends to move to an opt-out model of consent for cookies placed by websites. In practice, this would mean cookies could be set without consent on a website, but users would be given the option to block or delete cookies if they wish to. This would allow the government to maintain the current user experience and ensure the needs of processing cookie preferences. The opt-out model will be implemented by the DCMS and the ICO in due course.

Responses to the government's consultation highlighted that some value privacy and want control over how their personal data is used. To address this, the government will work with industry and the regulator on browser-based and similar solutions that will enable users to express their preferences. The government will also explore the forward proposals that require websites to respect automated signals notified by these technologies and will move to an opt-out model of consent for cookies only when the government ensures these solutions are widely available for use.

Direct marketing (question 2.4.9)

PECR rules on the use of electronic marketing messages for direct marketing. Currently businesses can contact individuals with whom they have previously been in touch during a sale or transaction with further marketing material about similar or related products and services, unless the individual has opted out. This is known as the 'soft opt-in' contact at the time they provided their details. This is known as the 'soft opt-in', and it does not require the customer's explicit consent.

The government asked for views on whether the soft opt-in should be extended to non-commercial organisations such as charities. The majority of respondents agreed with the proposal, noting that it would allow charities and other non-commercial organisations it would benefit, through greater rights groups seeked the could contact in larger volumes of unwanted communications.

Following consideration of responses, the government intends to extend the soft opt-in to non-commercial organisations. This will take place to make sure all appropriate safeguards are in place to protect individuals who do not wish to continue receiving communications.

Nuisance calls (questions 2.4.10, 2.4.11, 2.4.12, 2.4.13)

The consultation proposed measures to help the ICO to tackle rogue 'direct marketing' firms that are responsible for generating large volumes of nuisance calls, and extend a power to issue fixed penalties.

There was support for measures to allow the ICO to take enforcement action against organisations on the basis of the number of calls they generate (rather than purely on the basis of the number of complaints received by the ICO). Many respondents felt There was also support for the introduction of a 'duty to report' on communications providers, to require them to inform the ICO of suspicious levels of traffic on their networks.

The government plans to proceed with both proposals. In addition, the government is minded to lower the threshold at which the ICO can issue fixed penalties for large volume of nuisance calls of course. If the measures outlined here do not produce tangible results.

Bringing PECR enforcement regime in line with UK GDPR and DPA 2018 (questions 2.4.14, 2.4.17, 2.4.18)

The consultation also sought views on whether PECR should be amended to allow the ICO to take fines of up to £17m or 4% of a business's global turnover. The vast majority of respondents supported this proposal.

The consultation also asked views on whether the ICO should be able to serve assessment notices and carry out audits on organisations suspected of breaching PECR, in line with the provisions in UK GDPR and DPA 2018. The vast majority of respondents supported this proposal.

There was a general feeling amongst respondents that the current enforcement regime is not proportionate, and that the ICO should be able to issue more proportionate fines and use the suite of PECR audit organisations. Some respondents to the consultation called for greater harmonisation between the enforcement processes in PECR and those under the UK GDPR and DPA 2018.

The government agrees that there is scope for this, particularly as PECR's current enforcement regime is not in line with UK GDPR and DPA 2018 in relation to fines, data controllers and the regulator. The government therefore plans to proceed with these proposals.

2.5 Use of personal data for the purposes of democratic engagement

The government invited views on how PECR supports the democratic process. Currently, communications from political parties are treated as direct marketing. For example, political parties should not make automatic calls, email, or text the electorate unless they have obtained prior consent.

Communications for political campaigning (questions 2.5.1, 2.5.2)

The government sought views on whether the current rules governing political parties should continue to be subject to the same rules as commercial organisations from commercial organisations given the importance of democratic engagement to a healthy democracy.

The majority of respondents agreed that political communications should be treated PECR's rules on direct marketing. There were mixed views on whether to extend the soft opt-in to political parties and other political parties.

Those who supported the soft opt-in proposals noted that extending the proposal would allow political parties to communicate with their supporters of people to be reached and therefore lead to better engagement with politics. However, those who did not support the proposal felt that it would be inconsistent to treat with personal data.

The government plans to consider further whether political parties and campaigns should remain within the scope of PECR's direct marketing rules for democratic engagement purposes. The government recognises that political parties and campaigns have made exceptions to the direct marketing rules in the future Elections Act, it also intends to extend the soft opt-in rule to that political parties and elected representatives can contact individuals who have previously been in touch with them about a similar matter (for example, by attending a conference or making a donation) without their explicit consent, provided they have been given an opportunity to refuse such communications at the time their details were first collected. The government intends to do this as part of an opt-out of receiving communications from political parties and campaigns, in marketing communications from commercial organisations. This would allow political parties and elected representatives with organisations, which not already use the soft opt-in.

Lawful grounds for processing personal data under UK GDPR and DPA 2018 (questions 2.5.4, 2.5.5)

The government invited views on how the UK GDPR and DPA 2018 can be clarified to ensure that it is clear that it is lawful for political parties to use personal data for the processing of personal data for democratic engagement purposes falls within the public interest tasks lawful ground under Article 6(1)(e) of the UK GDPR. but there is uncertainty about this. Article 6(1)(e) of the UK GDPR provides a lawful ground for processing also identify a separate legal basis is law. This has sometimes been difficult for political parties and elected representatives, so the government asked for evidence from organisations on the barriers to effective political engagement and ways how the possible solutions.

The government also asked for views on paragraphs 22 and 23 of Schedule 1 to the DPA 2018 which set out the lawful processing of special category personal data without consent. Paragraph 22 states that political parties can process personal data about people's political opinions without consent, if it is necessary for the purpose of political activities for an individual who is a member of, or has regular contact with, Paragraph 23 states that elected representatives can process sensitive data without consent. when they have been asked to act on behalf of a constituent.

The majority of respondents disagreed that Article 9 of the UK GDPR provides the use of personal data for the purposes of democratic engagement. Around 9 was also noted that political parties and elected representatives have sector-wide of the UK GDPR and DPA 2018 are clearly in statute. One party said that it might be sensitive of processing of personal data for the purposes of democratic engagement, and that Schedule 1 of the DPA 2018 provides the use of sensitive data by an elected representative. Those who disagreed felt that the current provisions in the DPA 2018 are too restrictive for political activities (rather than when carrying out constituency casework) could be made clearer.

Having considered these responses, the government is minded to make some changes to Article 9 of the UK GDPR. to clarify the lawful grounds that can be relied upon by political parties and elected representatives. The government also intends to make representatives when processing personal data for the purposes of democratic engagement. The government also plans to amend paragraph 23 of Schedule 1 to the DPA 2018 to make it clear that it is lawful for elected representatives to process personal about political opinions for the purposes of democratic engagement in response to a request or PP undertaking a survey of local residents). Currently that condition only specifically refers to political parties, which causes unnecessary confusion.

2.6 Further questions

At the end of the chapter, the government posed for views on whether any of the proposals would impact on anyone with protected characteristics. Many respondents noted that the proposals would have a positive impact on those with protected characteristics. As outlined above, the government is not seeking to re-introduce a nominal fee for processing subject access requests, because it is concerned that this could disproportionately impact on those with vulnerable, including vulnerable people, and is not proceeding with the proposal to introduce a cost ceiling.

There was also some support for consolidating the UK GDPR, DPA 2018 and PECR, noting that it will lead to simplification of existing legislation. While the government agrees that the UK data protection regime is complex, it is worth noting that the primary is made now to clarify and improve areas of the current framework that are causing organisations the most difficulties.

Chapter 3: Boosting trade and reducing barriers to data flows

3.1 Summary

In chapter 3 of the consultation, the government set out that global networks of businesses, supply chains, and trade are increasingly underpinned by data flows. In chapter, the government sets out the importance of maintaining unnecessary barriers to cross-border data flows, including by proposing an ambitious programme of adequacy assessments.

The government intends to create an autonomous framework for international data transfers that reflects the UK's independent approach to data protection. that helps organisations to navigate the UK's data protection regime, and that supports cross-border business transactions and financial institutions. The UK's approach will be driven by outcomes for individuals and organisations. Continuing to ensure high standards of data protection will underpin the UK's approach to international data transfers. Reforms will allow the UK government and businesses to take an agile approach, recognising there are varying frameworks operating internationally that offer a high standard of data protection. The government also intends to remove unnecessary reduced burdens and clarify on how and where personal data can be transferred across borders.

A more agile approach to the international transfer regime will help domestic businesses to connect more easily with international markets, and attract investment from international firms looking to take advantage of the UK's commitment to personal data within the UK. Individuals will reap the benefits of organisations, hospitals and universities being able to share personal data quickly, efficiently and securely with their counterparts in other countries, helping to keep them safe internationally and socially connected to friends, families and communities around the world.

3.2 Adequacy

The government acknowledges that organisations currently face challenges and uncertainty when transferring personal data internationally.

Risk-based approach to adequacy (question 3.2.5)

The government proposed underpinning the UK's future approach to adequacy decisions with principles of risk assessment and proportionality.

Around half of respondents agreed with this proposal. Respondents thought that the proposed approach would be beneficial to organisations, because it would be more flexible and will minimise when making adequacy assessments. They felt that the proposed approach would support choices in the context of the impact of data protection standards.

The government will take forward reforms that further enable the UK to make adequacy assessments with a focus on risk-based decision-making and outcomes, and to keep the adequacy process under regular review. The UK's approach to adequacy regime will ensure the same broad standard that a country needs to meet in order to be found adequate, meaning individuals' data will continue to be well protected by a country with adequacy status. Organisations will benefit from a more flexible and agile data protection standards. The new UK regime that the GDPR has provided, but will also consider the desirability of facilitating international data flows when making adequacy decisions.

The government is respectful of countries' sovereign rights, and the different cultural approaches to data protection. The UK's data protection framework reflects our informed rights and recognise the contexts in which other countries operate, and take into account the impact of our decisions on other countries and their citizens.

Adequacy for groups of countries, regions and multilateral frameworks (question 3.2.2)

The government consulted on whether to make adequacy regulations for groups of countries, regions and multilateral frameworks. The majority of respondents agreed with the approach. Support was based on the greater interoperability that this approach would bring, and the benefits to UK businesses. Some respondents felt that a limited use or adequacy decisions will still need to consider the laws of each country, as recognised in the consultation document.

Adequacy regulations must be underpinned in the face of consistent developments to the legal landscapes of adequate countries. The government recognises the legacy of views, and assures that, if used appropriately, ongoing monitoring can safeguard data protection. The government will keep a close watch on the EU's approach to adequacy and ongoing monitoring process to meet the UK's formal review. The government therefore intends to proceed with repealing the requirement to review adequacy regulations every 4 years.

Redress requirements (question 3.2.6)

The government proposed to remove the requirement for assessing another country for adequacy. It is acceptable for that country to provide either administrative or judicial redress for UK data subjects, as long as the redress mechanism is effective. Around half of respondents agreed with the proposal, noting that it would be in line with the effectiveness of redress is more important than the form.

The government intends to proceed with this proposal. Under the reformed regime, the government will not specify the form in which redress should be provided. Instead, when conducting adequacy assessments, the government will consider the effectiveness of redress mechanisms available.

3.3 Alternative transfer mechanisms

Alternative transfer mechanisms provide a route for cross-border transfers of personal data to countries that are not subject to an adequacy decision. Many organisations rely on these alternative transfer mechanisms to make complex infrastructure to support such data sharing.

Proportionality of appropriate safeguards (questions 3.3.1, 3.3.2)

The UK GDPR sets out a list of safeguards, including standard data protection contractual clauses, to reinforce the importance of proportionality when assessing risk for alternative transfer mechanisms. The government called for views on support or challenge the proportionality of the current list of safeguards, including international transfer mechanisms, and whether it should be amended.

The majority of respondents agreed with this proposal, noting the challenges organisations face in assessing the risks of international transfers of personal data.

The government intends to proceed with this proposal. Under the reformed regime, the government will not specify the form in which redress should be provided. Instead, when conducting adequacy assessments, the government will consider the effectiveness of redress mechanisms available.

alternative transfer mechanisms. Respondents noted that the proposal would provide more clarity and support to more clearly and proportionately allow organisations to use alternative transfer mechanisms, without maintaining a high standard of protection for data subjects.

Reserve transfers (question 3.3.3)

The government proposed to remove reserve transfers from the scope of the international transfer regime. There were mixed views regarding this proposal. Those in favour noted that it would be helpful to remove reserve transfers from business or organisations without consequence to data protection.

However, there were mixed views on the extent of the positive impact on third party recipients. Those who disagreed with the proposed reform did so on the basis of the potential risk to data subject rights.

It was also noted that this reform will be complex and may not lead to a reduction in burden for organisations. Respondents also noted it agrees with the approval and therefore will not pursue legislative reform.

Adaptive transfer mechanisms (questions 3.3.4, 3.3.5, 3.3.6)

The government proposed allowing organisations to create or identify their own transfer mechanism. The majority of respondents disagreed with this proposal, on the basis that it would be too complex for SMEs and there was insufficient information about what is required for safeguarding transfers. Some expressed concern that the proposal may risk data protection standards. Respondents who supported the proposal noted it would provide more flexibility, remove complex and costly transfer requirements in some situations.

Given the absence of clear use cases for this proposal, the government will not pursue this approach.

A power to create alternative transfer mechanisms (questions 3.3.7, 3.3.8)

The government proposed creating a new power for the ICO/Secretary of State to formally recognise new alternative transfer mechanisms, which would allow the ICO/Secretary of State to recognise transfer mechanisms from other jurisdictions or recognise in UK law other international data transfer mechanisms. If they achieve data outcomes required by UK law.

There were mixed views on this proposal, with support for the opportunities for interoperability and future-proofing, but some concern about the potential risk that new mechanisms could lower data protection standards.

The government recognises the mixed views on this issue, but assesses that this reform will help to future-proof the UK's approach to international transfers by allowing the UK to recognise new international transfer mechanisms. The government will pursue this reform forward and ensure that new mechanisms must meet the same high data protection standards as the other alternative transfer mechanisms.

3.4 UK certification schemes

Certification schemes are voluntary, market-driven frameworks of control specific rules and criteria, that allow organisations to demonstrate their compliance with data protection and provide appropriate safeguards for international transfers. They are characterised by external or the sectoral or industry level, defining data protection rules and criteria for organisations, products, processes and services within the scheme that sector, industry or similar group.

However, certification schemes are complex measures that require significant time and resources to design, implement and maintain, and demonstrable accountability for the data protection outcomes they achieve. The government proposed that this would provide for a more globally interoperable market-driven system that better supports the use of certification as an alternative transfer mechanism.

Assessing certification schemes to increase interoperability (questions 3.4.1, 3.4.2)

To facilitate compatibility with a wider range of personal data protection regimes, the government proposed that the ICO would be able to assess certification schemes against different approaches to accountability, such as privacy management programmes, and secondly to clarify that certification bodies outside the UK can be recognised by UK certification schemes as competent bodies.

There were mixed views on both proposals. Respondents noted that the reforms may benefit UK businesses by facilitating easier personal data flows. Other respondents were less sure that these proposals would benefit them or their organisations.

Supporting interoperability is important for organisations. However, there remains a lack of evidence on how these reforms will lead to increased uptake. The ICO will monitor, at this time, whether the proposed reforms are the best way to deliver greater interoperability. The government will consider other approaches to meeting this goal.

3.5 Derogations

The consultation set out that the current overarching approach to the use of derogations is working well. However, the ICO should provide more guidance they are necessary and where neither adequacy nor other safeguards are appropriate. As outlined in this section of the consultation, technical changes may help to clarify the restrictions on using derogations.

Repetitive use of derogations (question 3.5.1)

The government proposed removing the requirement for formal review in flexibility for the use of derogations, by making explicit that repetitive use of derogations is permitted. There was some opposition to this proposal, with respondents expressing concerns that it would be too complex for SMEs to use. There was also concern from some respondents agreeing that it would represent a proportionate increase in flexibility for transfers. The government will not pursue this reform.

3.6 Further questions

At the end of the chapter, the government asked for views on whether any of the proposals would impact on anyone with protected characteristics. There were no specific concerns related to the impact any proposals would have on those with protected characteristics; we were there significant issues raised by respondents in response to the rest of the chapter's proposals.

The consultation posed some open-ended questions at the end of this chapter to respondents to provide any other comments on the proposed reforms. Respondents raised a number of concerns about the proposed reforms to the UK GDPR, including that the reforms, particularly those with protected characteristics. The protection of people's personal data is already at the heart of the UK's data regime and will continue to be as the government embarks on its reform agenda.

Chapter 4: Delivering better public services

4.1 Summary

In chapter 4 of the consultation, the government highlighted the opportunities to hold data processing for public services, the ability to share personal data for research in the public interest, and the benefits of collaboration between the public and private sectors in all parts of the United Kingdom.

There are currently some challenges to doing this effectively, including:

- data infrastructure that is not interoperable
- data quality issues and duplication
- inconsistent data capability in the workforce
- financial disincentives that discourage investment

The government wants to create a joined up and interoperable data ecosystem for the public sector across the whole of the UK, that will address the limitations outlined above and drive better use of data. This will lead to better public services and better improve the delivery of government services through better use and sharing of personal data, including data sharing across the whole of the UK.

4.2 Digital Economy Act 2017

Part 5 of the Digital Economy Act 2017 allows personal data sharing to support services for the benefit of individuals in England, Wales and Northern Ireland. The government, Universal public services, the government sought views in the consultation to extend the public service delivery powers under section 35 of the Digital Economy Act 2017 to support the delivery of services for the benefit of businesses, including by using digital verification services, or accessing support when trying to set up new businesses.

Extend powers under s 35 of the Digital Economy Act 2017 (question 4.2.1)

There were mixed views on this proposal. Around a third of respondents agreed, noting that it would be helpful to use data to support businesses to access services, set them, such as identity verification services, accessing support when starting a new business, or applying for government grants and licences. Around a third of respondents disagreed, noting that it would be better to use data to provide support by government bodies or that the proposal would allow the government to share personal data with businesses. However, a similar number of respondents were neutral towards this proposal.

The government recognises the balance of views on this proposal. The government will consider how it can support the use of digital verification services and support data sharing within the public sector to improve public services, such as facilitating personal data sharing from the public to the private sector for other reasons. Any proposals will be subject to further consultation and parliamentary scrutiny.

4.3 Personal data use during the COVID-19 pandemic

Section 10 of the Digital Economy Act 2017 provides for the public, private and voluntary bodies to disclose personal information, specifically for the purposes of improving public health. The current legislation has generally not prevented such processing from taking place, but the consultation sought views on whether any aspects of the legislation could be made clearer.

Non-public bodies delivering public health functions (questions 4.3.1, 4.3.2)

The consultation identified the under-reliance on the public task lawful ground (Article 6(1)(e) of the UK GDPR) by non-public bodies delivering public health functions, and where a non-public body is processing personal data in order to help a public body to perform its public task, it may be able to rely on the public task lawful ground. However, if a third party is asked by a public body to help it to perform its public task, it may be unclear whether it can do so. In some circumstances, it is clearly appropriate for a third party to act as a processor for a public body, and in other circumstances it may be appropriate for the third party to rely on the legitimate interests lawful ground under Article 6(1)(f) of the UK GDPR in the circumstances of the particular case. However, it may not be clear to the third party that data processor on behalf of the controller under a formal data processing arrangement.

To address uncertainty in this area, the government proposed to clarify that private organisations and individuals seeks to carry out an activity at the request of a public body may rely on that body's lawful ground for processing the personal data under Art 6(1)(e).

The majority of respondents agreed with this proposal, although respondents noted the importance of ensuring that the data subject is informed about who is using their data. Individuals, for example, several respondents asked if individuals would still have the right to object to their personal data being used for a public task if the proposal was enacted. Some respondents raised concerns regarding it a pandemic or the prevention of crime and serious crime, and whether the proposal would mean that personal data could be applied to any situation where a non-public body was asked to carry out a government department, local authority or other public body to help deliver a service.

Respondents were seen supposed to the proposal said that legislative changes would not be required if public bodies entered a formal contribution processor agreement with non-public bodies. Some of the respondents who disagreed with the proposal noted that public should continue to rely on the lawful ground of legitimate interests.

Having considered the responses, the government plans to introduce legislation to clarify which lawful grounds for processing are available for organisations under Article 6 of the UK GDPR when they are requested by a public body to help deliver a public task.

Processing health data in an emergency (questions 4.3.3, 4.3.4)

The government proposed that it would be helpful if the processing of the healthcare sector were clear about what conditions in Schedule 1 to the UK GDPR they could rely on when processing health data for the purposes of public health.

The majority of respondents agreed that greater clarity in the legislation would be helpful. However, a number of healthcare organisations and patients' groups advised caution, noting that the sensitive nature of health data and the importance of healthcare sector could process sensitive information about people's health.

They pointed to the existing exemption in paragraph 3 of Schedule 1 to the DPA 2018, which provides a condition for processing health data for public health purposes, subject to a duty of confidence apply. This should be read in conjunction with Schedule 1 which sections have a duty of confidence may arise. In addition, some respondents who disagreed with the proposal noted that it would be helpful to have more guidance and flexible, which they regard gave them a clear legal basis for sharing personal data with the relevant healthcare authorities in certain situations during the pandemic.

Having considered the arguments for and against, the government does not intend to pursue this proposal.

4.4 Building trust and transparency

Public trust is vital to the delivery of better public services and outcomes for everyone. It is also vital for the UK's ability to use data to drive innovation in consumer public bodies to share and utilise algorithmic tools to improve efficiency and service delivery. Many citizens are concerned about the use of their data by public bodies.

Transparency mechanism for algorithms (questions 4.4.1, 4.4.2, 4.4.3)

Increasing transparency of the use of algorithms, factors for decision making in the public sector was proposed in the consultation. This would increase accountability and enable compulsory transparency reporting on the use of algorithms in decision-making for public sector bodies.

The majority of respondents agreed with this proposal, with respondents outlining they would support the proposal to mandate transparency reporting. Respondents noted it would also improve accountability, especially if the reporting includes accountability mechanisms such as redress. Some respondents who disagreed with the proposal noted importance of transparent information being presented in an accessible, interpretable and meaningful way to the general public. Responses included a wide range of suggestions on the contents that should be included in the mandatory reporting requirement.

The recently launched Algorithmic Transparency Standard encompasses the categories recommended for transparency reporting during the consultation process. This includes providing information on:

- how teams are using the algorithms tool
- why they are using the algorithms tool
- the benefits and risks associated with the algorithmic tool
- the purpose of the tool
- how the tool affects decision-making
- the technical specifications of the tool and dealing the tool
- information about the risk and impact assessments conducted

The government does not intend to take forward legislative change at this time due to the early stage of this work, but remains strongly committed to algorithmic transparency and will continue to pilot and gather feedback on the standard and explore policy enforcement options in the future.

The consultation asked an open question about whether any exemptions should apply to the proposed transparency reporting requirement. The majority of respondents noted that by requirements. Many stated that no exemptions should apply whatsoever, whereas others believed that a limited exemption might be needed in areas such as national security or law enforcement.

The government will therefore continue to consider the case for exemptions as part of the piloting of the Algorithmic Transparency Standard, overall providing much greater transparency on the use of algorithms in the public sector. The specifications of the algorithms, and technical considerations (such as intelligibility bias) are addressed. The government also recognises respondents' views on whether there should be a requirement for a mandatory transparency reporting tool and will consider recommendations from the consultation response in the future in this area.

Processing in the substantial public interest (questions 4.4.4, 4.4.5, 4.4.6, 4.4.7)

As outlined in the consultation, sensitive personal data cannot be processed unless one of the conditions in Article 9 of the UK GDPR is met. Sensitive personal data processed under Article 9(2)(g) UKGDPR can be lawful if it is strictly necessary and proportionate to balance between ensuring processes are sufficiently flexible to allow all necessary processing to take place, while ensuring processes are specific enough to give data subjects transparency and controllers certainty.

There were mixed views on whether there are situations involving the processing of sensitive data that are not adequately covered by the current lawful ground in the UK GDPR and Schedule 1 to the DPA 2018. However, the majority of respondents agreed that the current lawful ground in Schedule 1 to the substantial public interest framework processing that is not public interest.

To address this, the government proposed including in legislation a definition of 'substantial public interest' and offered to include examples in Schedule 1 to the UK GDPR and Schedule 1 to the DPA 2018. However, the majority of respondents agreed that the current lawful ground in Schedule 1 to the substantial public interest framework processing that is not public interest.

To address this, the government proposed including in legislation a definition of 'substantial public interest' and offered to include examples in Schedule 1 to the UK GDPR and Schedule 1 to the DPA 2018. However, the majority of respondents agreed that the current lawful ground in Schedule 1 to the substantial public interest framework processing that is not public interest.

The majority of respondents supported the introduction of a definition of substantial public interest. Respondents recommended that any definition must list far too narrow and too broad. Respondents also noted that there was also concerned that the definition could be very difficult to define.

The government has considered how to devise a definition of substantial public interest, but does not believe a definition would add value and cover the range of activities that are required at this time. Furthermore, the government concluded that it would be difficult to define in a way that is sufficiently comprehensive and that it already effectively creates data controllers to consider the specific benefits of their processing to the wider public and ensures controllers evaluate the necessity of their processing. For this reason, the government has decided not to define substantial public interest at this time.

Around half of respondents agreed that there may be a need to add to, or amend, the list of Schedule 1 conditions in the DPA 2018. The government considered the situations raised with great interest. However, the government is not currently considering expanding the list in Schedule 1 to the DPA 2018 would pose too great a risk to privacy and data rights.

The government is currently going further though by these proposals, including amendments to the substantial public interest condition. The government is also adding a condition in Schedule 1 to allow them to carry out some routine administrative duties. The government is also considering proposals from sports bodies that would prevent a person who has been convicted of a sexual offence from participating in sport. It is also a suggestion from one respondent that companies which currently prevent the processing of race and ethnicity data to improve diversity at senior levels within companies could be extended to other types of data relating to underrepresented groups.

Clarifying rules on biometric data in policing (question 4.4.8):

Technologies such as DNA and fingerprint analysis, and, increasingly, facial image recognition, are important public safety tools for the police. The public rightly expects the police to use these tools within a framework that ensures accuracy and fairness and proportionality.

There is an existing lawful framework for the police to use biometric technologies to support their operational activities, including the processing of data. The UK GDPR framework is among strong protections, which means it is sufficiently flexible to allow for its applicability to new technologies. However, it can be complex and difficult for both the police and the public to understand the protections of organisations' rights and respect privacy, human and equality rights.

The majority of respondents supported improving the clarity of the existing legal framework. A majority felt that certain technologies, such as facial recognition, required specific legislation. However, others agreed that a principle-based approach would provide greater flexibility to future developments. The majority of respondents felt some highlighting the risk that specific legislation could hinder law enforcement from adoption of new technology to protect the public. Several respondents also said that the current UK GDPR framework is sufficient to cover the use of biometrics.

Evidence from the consultation also suggested that implementation challenges can not limited to the use of biometric capabilities, but are common to the police's adoption of new tools and technologies. Recommendations from the consultation response included consultation and wider stakeholder engagement, the government recognises the benefits for the police and public from greater clarity on how the police can and should use biometric technologies, and will explore how to provide greater clarity and building public understanding, support and trust when these technologies are being developed and used.

The government will work with policing authorities to promote high standards and best practice for the responsible and fine use of new technologies, including supporting the National Biometrics Commissioner to develop his new codes of practice, as set out in section 20 Trustworthy safety and national security.

A small number of respondents suggested greater consistency between the rules around different types of biometrics. The government is considering the consultation response and will explore how to provide greater clarity and consistency in the rules and images with those for DNA and fingerprints, with an exception that similar rules would apply to any other biometrics in future.

4.5 Public safety and national security

The effective sharing of personal data for law enforcement and national security purposes is vital to the work of our law enforcement bodies and UK intelligence services, and is in the interests of public safety. To drive consistency across the UK and EU, the UK GDPR and Law Enforcement Directive (LED) provisions governing processing of the Data Protection Act 2018. the government proposed to clarify whether it is possible to align key terms that are used across these different data processing frameworks.

The majority of respondents agreed with this proposal, stating that it will provide greater clarity and consistency. However, a number of respondents also highlighted that it is important to recognise where or how the two regimes deliberately impose differing obligations on those processing under them. The government recognises that the UK GDPR and the Law Enforcement Directive (LED) contains a definition of consent, but there is no equivalent definition under Part 3 of the Data Protection Act 2018. The government is therefore considering introducing this to provide clarity and consistency.

Another example where the government could create consistency across regimes is in regard to codes of conduct. In the UK GDPR, these can be produced by representative bodies to aid the effective application of the GDPR, taking into account the needs of particular sectors, which are then approved by the ICO. There is currently no equivalent power under Part 3 of the Data Protection Act 2018. The government is considering whether to introduce a power for the Secretary of State to approve codes of conduct, to have the same ability as other sectors. In line with the feedback received from respondents, the government will ensure that any changes are clear, to prevent further confusion.

4.6 Further questions

At the end of the chapter, the government posed no views on whether any of the proposals would impact on anyone with protected characteristics. There were no specific concerns related to the impact any proposals would have on those with protected characteristics; we were there significant issues raised by respondents in relation to the questions and topics in this chapter.

The consultation posed some open-ended questions at the end of this chapter for respondents to provide any other comments on the proposed reforms. Respondents highlighted the importance of protecting personal data when these reforms come into force, particularly those with protected characteristics. The protection of people's personal data is already at the heart of the UK's data regime and will continue to be as the government embarks on its reform agenda.

Chapter 5: Reform of the Information Commissioner's Office

5.1 Summary

In chapter 5 of the consultation, the government explored proposals to reform the Information Commissioner's Office. The ICO plays a critical role in an increasingly data driven economy. It is important that the ICO is a modern regulator, fit for the future and suitable for world-leading reputation. The proposed reforms sought to better equip the ICO in performing its function as an agile and forward-looking regulator, by ensuring it has a modern governance framework, leading to a clearer mandate for a risk-based and proactive approach to its regulatory activities.

Specifically, the government set out how it intends to improve the legislative framework that underpins the ICO by:

- setting new and improved objectives and a clearer strategic vision for the regulator
- changes to its governance model, improving accountability mechanisms, and ensuring it is fit for a modern regulator
- 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 personal data use

The ICO is currently a non-departmental public body, and it will be more clearly required to take a risk based and proactive approach, focusing the highest risks and harms in its activities while helping organisations comply with the law from the outset, rather than focusing on punishing them after they have breached the law. The ICO's new objectives need to be more transparent, so that Parliament and the public can more easily track the ICO's account as to whether it is meeting its responsibilities.

5.2 Strategy, objectives and duties

Currently, the UK GDPR does not provide the ICO with a clear framework of strategic objectives to underpin its regulatory activities. This makes it difficult to measure its performance and be held accountable by its stakeholders. Instead, the ICO is obliged to fulfill a long list of duties and functions, as set out in Article 57 of the UK GDPR, but without a strategic framework to guide its work.

The government proposed introducing a new, statutory framework that sets out the ICO's strategic objectives, which would sit at the top of its governance model and guide its protection functions. A clearer set of statutory objectives and duties for the ICO will offer greater clarity and stability to the ICO's crucial and public interest functions, and provide accountability to Parliament and public of what the regulator is.

A new statutory framework for the ICO (question 5.2.1)

Almost half of respondents agreed that the ICO would benefit from a new statutory framework for its objectives and duties. Respondents indicated that the reforms would provide more clarity and focus for the ICO, improve accountability for its powers, duties and objectives. Respondents also noted that a new statutory framework would provide a stronger basis for the ICO to focus on transparent decision-making, and would help to underpin its independence. There were some disagreement with the proposal, with respondents expressing concern about the potential loss, perceived or real, to the ICO's independence, and arguing that the current framework is sufficient.

The government recognises these views, particularly the concerns expressed by consultees around independence, and has carefully considered the need to maintain the independence of the ICO when taking forward reform. The government intends to proceed with the proposal to introduce a new statutory framework. Some and outlines, but with some changes to the original proposals which are set out below.

To ensure clarity on how the objectives and duties are to operate alongside the ICO's existing functions and tasks, the new framework will be designed in a way that ensures the ICO's duties to uphold data protection and promote data protection, promote the responsible personal data use, while also having regard to growth and innovation, competition, and public safety.

Overarching objective (question 5.2.2, 5.2.3)

The government proposed to introduce a new overarching objective for the ICO with 2 elements: ensuring data protection is upheld to a high standard, and promoting responsible personal data use. The majority of respondents supported this proposal.

Some of those who agreed highlighted that the overarching objective aligns with the ICO's current mission, and promoting it in law would provide a welcome step, allowing the ICO to ensure that, on a statutory basis, individuals' personal data is protected, whilst organisations can innovate using data. However, a number of respondents disagreed with the proposal, some argued that the ICO's primary duty should be to protect people's data rather than promoting its use, and argued that a new principle objective or duty would be required to balance the new objective.

The government plans to proceed with the proposal to introduce a new principal objective for the ICO. The government will also seek to ensure that the ICO takes a proportionate, risk-based approach to enforcing its objectives.

Sitting below the principal objective, the government will introduce specific statutory duties for the ICO to ensure it pursues its new objectives in a clear, transparent and open way. These duties will strengthen the ICO's existing obligations and ensure it is equipped to factor in interactions with other duties.

Growth, innovation and competition duties (questions 5.2.4, 5.2.5):

The government proposed to introduce new statutory duties to empower the ICO to promote growth and innovation to other domains as it supervises and enforces the UK's data protection regime.

The majority of respondents disagreed with the proposal to introduce a growth and innovation duty. Respondents raised concerns that the duty would pose a conflict of interest for the ICO between its primary objective of upholding data rights, and having a duty to promote growth and innovation. Some felt that the ICO should focus on itself with impacts on growth and innovation, and should instead focus only on data protection matters.

There were a minority of respondents disagreed with the proposal to introduce a competition duty. As with the growth and innovation duty, concerns were raised that a competition duty would create a conflict of interest for the ICO regarding its primary objective.

However, in both cases, respondents who agreed with the proposals cited that the ICO should consider growth and innovation, and competition when considering and discharging its functions. for example to the ICO's existing collaboration with the Competition and Markets Authority, and that the proposals will formalise existing collaboration between the ICO and other regulators, and ensure consistent and effective regulatory conflicts activity. Those who agreed with the proposals also highlighted the importance to the overarching objective to take precedence if the ICO's duties to promote growth, innovation and competition conflict.

The government sees the ICO's role in ensuring responsible data protection, innovation and economic growth, and therefore intends to ensure that the regulator is required to have regard to competition, growth and innovation.

Public safety duty (question 5.2.6):

There were mixed views regarding the proposal to introduce specific language recognising the need for the ICO to have regard to public safety when exercising its functions. Those who disagreed with the proposal noted that the ICO already has a duty to have regard to law enforcement and public safety and national security and rights and freedoms of individuals.

The government is not introducing a duty to ensure the ICO also has regard to public

Statement of strategic priorities (question 5.1.1)

The government proposed to introduce a power for the DPCMS Secretary of State to issue a statement of strategic priorities (SSP) for the ICO to have regard to in discharging its data protection functions. The majority of respondents disagreed with this proposal. Concerns were raised that this measure would pose a risk to the ICO's independence and regulatory powers. Respondents felt that the SSP could be used to limiting the parameters of the SSP so that it would only perform relating to the public sector.

The government plans to proceed with the power to introduce an SSP as it will be a transparent way for the government to set out the priorities or objectives it is providing the ICO with under consent. Given the government's commitment to ensuring that the ICO's independence is not affected, the SSP will not be mandatory for the ICO under the UK GDPR and the DPA 2018. While the ICO will be required to respond to the priorities contained in the SSP, the ICO will not be legally bound to act in accordance with the priorities contained. Further, the SSP will be subject to parliamentary scrutiny before it is designated.

Collaboration and enhanced information sharing gateways (questions 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5)

The majority of respondents agreed with the proposal to introduce a duty for the ICO to collaborate and share information with other regulators. Respondents felt that this proposal will help prevent ex-parteing and improve cooperation between regulators. Respondents who agreed with the proposal also highlighted that the duty will ensure consistency across the regulatory landscape. However, a minority of respondents that disagreed argued that the duty would constitute the regulatory landscape.

The government will amend the proposal to introduce a duty for the ICO to cooperate and consult with other regulators. The ICO already has mechanisms in place which allow for close cooperation with other regulators, primarily through Memoranda of Understanding. The ICO has also been proactive in setting up informal networks for the ICO to consult with relevant regulators and any other relevant bodies when exercising its duties to have regard to growth, innovation and competition.

The government will proceed with the proposal to introduce enhanced information sharing gateways for the ICO. Some suggested that an improved information sharing gateway would help regulators standardise a consistent regulatory approach. Others highlighted that the ICO's ability to share information has to fits the aim that the case for an enhanced information sharing gateway was unclear.

The government will not continue with the proposal to introduce an enhanced information sharing gateway as we believe the ICO's existing information sharing powers are sufficient.

The ICO's international role (questions 5.3.1, 5.3.2, 5.3.3)

As part of the new statutory framework, the government proposed the introduction of a new strategic objective for the ICO to "promote the UK's data protection interests and priorities when conducting its own international activities. The majority of respondents disagreed with this proposal, with risks to the ICO's independence consistently raised as a key concern. Respondents felt that this proposal could run risks to the ICO's international reputation and the UK's adequacy status.

The government will not continue with the proposal to include an international objective for the ICO. Instead, the government may state its international priorities and data policy in the SSP. Setting government priorities out in a public statement will ensure that the ICO's independence is not at risk, it is in line with such other data priorities for international work.

Around half of respondents supported the proposal to require the ICO to deliver a more transparent and structured international strategy. Instead, the government will pursue this proposal without interfere the ICO's accountability. Respondents also disagreed with the proposal to place independence concerns.

The government will not continue with the proposal for the ICO to deliver a more transparent and structured international strategy. Instead, the government will pursue this proposal without interfere the ICO's independence. Respondents also disagreed with the proposal to place independence concerns.

There were mixed views on the proposed changes to governance roles for the regulator. While some of those in support acknowledged that a change in the governance model would bring the UK in line with other regulators, others raised concerns about the ICO's independence or that they saw no issue with the current model.

The government recognises the balance of views in this proposal and believes that having powers and responsibilities spread across a board, rather than with one individual, should ensure greater independence and integrity. The government does not agree that the ICO's independence is currently compromised by its governance model, the current model has been in place since the regulator's establishment in 2018 and the ICO has grown significantly in size and importance. The government wants to ensure it is fit for the future and believes that the ICO is now in a time with such a large, and therefore intends to proceed with this proposal.

Appointments process (questions 5.3.3, 5.3.4, 5.3.5, 5.3.6)

The consultation outlined the government's proposed processes for the statutory roles of the new governance model. This was to ensure that, in the same process as the Government's Public Appointments process, it complies with the Government's Public Protection Act 2018. This means that the chair would be appointed by Her Majesty's Letters Patent, following a recommendation from the government based on merit, after a fair and open competition. The majority of respondents agreed that the chair and executive members of the ICO's future board and its chief executive officer should be appointed by the DCMS Secretary of State as the public appointment process.

There were mixed views on the proposed changes to the appointment process for the rest of that, the proposed appointment process for the non-executive members of the ICO's future board and its chief executive officer should be appointed by the Secretary of State. Respondents believed that a fair and open process was important to ensure the best candidates for the roles. Respondents also highlighted the importance of the independence of the regulator, particularly for the role of chief executive.

Following the views outlined above, the government intends to retain the current Information Commissioner appointment process (by Her Majesty by Letters Patent) for the chair of the ICO, as it is in line with the Government's Public Protection Act legislation. The government believes that the public appointment process for the non-executive members of the board has sufficient safeguards to protect the ICO's independence and will ensure a fair and open process. The government believes that the appointment processes are governed by the Governance Code for Public Appointments, regulated by the Commissioner for Public Appointments. The balance between independence and accountability is also maintained by the role of the government and Parliament. The government proposes that, in line with regulatory plans, intends to appoint the non-executive members as the public appointment process.

Acknowledging that chief executive roles are more commonly appointed by the board, the government will not appoint the role of chief executive as the public appointment process. Instead, the chief executive of the ICO will be appointed by the ICO's board in consultation with the DCMS Secretary of State.

Information Commissioner's salary (question 5.3.7)

The current legislation requires parliamentary approval to amend the Information Commissioner's salary. The majority of respondents agreed that, in the future, governance model, the government proposed to remove this requirement. There were mixed views on this proposal, with around a third of respondents being neutral, a third in agreement and a third in disagreement. Those who were in agreement stated that parliamentary scrutiny was helpful, and removing this requirement could lead to a lack of transparency. Others felt that it would increase or decrease the salary in direct response to the individual's performance.

The government does not see the ability to amend the salary of any of the new statutory roles in the proposed governance model as a way to directly incentivise certain behaviours. The ability to set salary is a key lever for the board to use to attract the remuneration necessary to attract and retain the best possible candidates. Under the governance model change, the removal of this requirement would bring this in line with other regulators' salary setting. The Information Commissioner's salary is currently Public consultation salaries over £150,000 are approved by the Treasury's Senior Salaries Review Body (SSRB). The government believes this sufficient safeguard ensures that the salary is in line with other public sector salaries. The government therefore intends to proceed with the removal of this requirement.

Name of the Information Commissioner's Office (not included in the consultation)

Given the change in governance model, the name of the regulator (being the "Information Commissioner's Office" may no longer accurately reflect the organisation, as it will not be the office of one individual.

To ensure that the name of the body is not misleading, the government is considering options for a new name for the regulator.

5.4 Accountability and transparency

As set out earlier in this chapter, there is a lack of clarity around the ICO's strategic priorities in the current legislative framework. This means that there are no clear objectives for the ICO to measure its performance against and report on. The government proposes to place a duty on the Secretary of State to prepare statements for the ICO, to set strategic priorities of the ICO's performance.

Now reporting requirements (questions 5.4.1, 5.4.2, 5.4.3, 5.4.4, 5.4.5)

The majority of respondents agreed with the proposals to strengthen the ICO's reporting requirements. Respondents felt this would increase the accountability of the regulator and would lead to a better understanding of the ICO's activities. Respondents also disagreed believed that the ICO already had sufficient reporting requirements in place and that this could cause unnecessary bureaucracy.

The vast majority of respondents agreed with the proposal to require the ICO to publish the key strategies and processes that guide its work. These to have feel that this would increase transparency and would be a helpful tool for businesses and other regulators. Respondents also disagreed recognised that the ICO already publishes many documents and that further publishing requirements for the regulator would add red bureaucracy.

The majority of respondents supported the proposal to introduce a requirement for the ICO to develop and publish comprehensive key performance indicators. Respondents felt this would increase the accountability of the regulator, ensure its effectiveness and provide evidence of how the ICO is meeting its statutory obligations. Respondents who disagreed believed the current reporting mechanisms in place are sufficient.

The government plans to proceed with introducing regulatory measures for the ICO to report on its approach and performance. In particular, the ICO will be required to publish:

- **A strategy setting out how it will discharge its functions and deliver against its strategic priorities.** The ICO will be required to report annually on performance against its strategy.
- **Key Performance Indicators (KPIs).** The ICO will be required to report at least annually against its KPIs.
- **An approach to delivering its new objectives and duties framework.** The ICO will be required to report annually on how it has discharged its functions in line with the new framework (discussed in section 5.3 Ministerial objectives and duties).
- **A response to the government's Statement of Strategic Priorities** outlining how it has taken into account the government's priorities. The ICO will be required to report annually on activities taken, as set out in the response to the Statement (discussed in section 5.3 Ministerial objectives and duties).
- **An approach to enhanced consultation and setting up expert panels with regards to codes of practice and statutory guidance.** The composition of the panel will depend on the subject matter being consulted on and will include a mix of panel members. A summary of their engagement should be published alongside a justification for why the ICO has or has not adopted recommendations from the panel. The government will also consider how the ICO's approach to setting statutory guidance should also be established (discussed in section 5.5 Codes of practice and guidance).
- **An approach to overcoming its discretionary concerning complaints handling** (discussed in section 5.6 Complaints).
- **Statutory guidance under s.160 of the Data Protection Act 2008,** which will be extended to include the ICO's law enforcement powers.

The ICO will also be required to report annually on its approach to enforcement and use of its powers. This should include information on its approach to exercising its law enforcement powers, and, the timeframes for all completed investigations and the outcomes of the investigation process.

Independent review (questions 5.4.6, 5.4.7)

In certain circumstances, the government may wish to assess the ICO's performance against its strategic priorities. The majority of respondents agreed with the proposal for an independent review. Respondents felt this would increase the accountability of the regulator and would lead to a better understanding of the ICO's activities. Respondents also disagreed believed that the ICO already had sufficient reporting requirements in place and that this could cause unnecessary bureaucracy.

The vast majority of respondents agreed with the proposal to require the ICO to publish the key strategies and processes that guide its work. These to have feel that this would increase transparency and would be a helpful tool for businesses and other regulators. Respondents also disagreed recognised that the ICO already publishes many documents and that further publishing requirements for the regulator would add red bureaucracy.

The majority of respondents supported the proposal to introduce a requirement for the ICO to develop and publish comprehensive key performance indicators. Respondents felt this would increase the accountability of the regulator, ensure its effectiveness and provide evidence of how the ICO is meeting its statutory obligations. Respondents who disagreed believed the current reporting mechanisms in place are sufficient.

The government plans to proceed with introducing regulatory measures for the ICO to report on its approach and performance. In particular, the ICO will be required to publish:

- **A strategy setting out how it will discharge its functions and deliver against its strategic priorities.** The ICO will be required to report annually on performance against its strategy.
- **Key Performance Indicators (KPIs).** The ICO will be required to report at least annually against its KPIs.
- **An approach to delivering its new objectives and duties framework.** The ICO will be required to report annually on how it has discharged its functions in line with the new framework (discussed in section 5.3 Ministerial objectives and duties).
- **A response to the government's Statement of Strategic Priorities** outlining how it has taken into account the government's priorities. The ICO will be required to report annually on activities taken, as set out in the response to the Statement (discussed in section 5.3 Ministerial objectives and duties).
- **An approach to enhanced consultation and setting up expert panels with regards to codes of practice and statutory guidance.** The composition of the panel will depend on the subject matter being consulted on and will include a mix of panel members. A summary of their engagement should be published alongside a justification for why the ICO has or has not adopted recommendations from the panel. The government will also consider how the ICO's approach to setting statutory guidance should also be established (discussed in section 5.5 Codes of practice and guidance).
- **An approach to overcoming its discretionary concerning complaints handling** (discussed in section 5.6 Complaints).
- **Statutory guidance under s.160 of the Data Protection Act 2008,** which will be extended to include the ICO's law enforcement powers.

The ICO will also be required to report annually on its approach to enforcement and use of its powers. This should include information on its approach to exercising its law enforcement powers, and, the timeframes for all completed investigations and the outcomes of the investigation process.

Independent review (questions 5.4.6, 5.4.7)

In certain circumstances, the government may wish to assess the ICO's performance against its strategic priorities. The majority of respondents agreed with the proposal for an independent review. Respondents felt this would increase the accountability of the regulator and would lead to a better understanding of the ICO's activities. Respondents also disagreed believed that the ICO already had sufficient reporting requirements in place and that this could cause unnecessary bureaucracy.

The vast majority of respondents agreed with the proposal to require the ICO to publish the key strategies and processes that guide its work. These to have feel that this would increase transparency and would be a helpful tool for businesses and other regulators. Respondents also disagreed recognised that the ICO already publishes many documents and that further publishing requirements for the regulator would add red bureaucracy.

There were mixed views on the proposal. Respondents who agreed highlighted the importance of the ICO being subject to scrutiny, while those who disagreed cited concerns around the impact on the ICO's independence.

The government recognises the balance of views on this issue and the importance of independence for the regulator. The government does not agree that this is in line with the proposal to empower the Secretary of State to initiate an independent review, particularly given the other current non-legislative mechanisms available. The process for this follows the Cabinet Office guidance on reviews of non-departmental public bodies.

5.5 Codes of practice and guidance

The DPA 2018 requires the ICO to prepare codes of practice on four specified data protection matters, including the ICO's own practices for complying with data protection and practice for organisations. The DPA 2018 requires the Information Commissioner to consult the DCMS Secretary of State, and any other individuals and organisations she considers appropriate by the Commissioner, before preparing or amending these of the code.

The ICO is also required to lay such published statutory guidance on various areas, for example, its regulatory action, and is required to consult the Secretary of State and other appropriate persons when doing so. In addition to codes of practice and other statutory guidance, the ICO also has a duty to provide data protection guidance and powers to develop and publish non-statutory guidance on processing activities that need to data protection.

The ICO's current provision of practice and guidance on complex and technical areas, smaller organisations which do not have large compliance divisions. It can be particularly challenging to understand and comply with such codes of practice and guidance. Stakeholders also felt that the ICO's current approach to developing such codes, and non-statutory guidance is notable indicative of what the Information Commissioner considers to be good practice and may also be taken into account by the courts and tribunals when considering whether a data controller has complied with its practice. As such, it is crucial that the ICO's codes of practice and guidance are accessible and enable regulated persons to comply with the expiration of priority and clarity.

Requirement to carry out impact assessments (question 5.5.1)

The government proposed that the requirements for the ICO to undertake and publish impact assessments when developing codes of practice and guidance on complex or novel issues. Whilst the ICO already carries out impact assessments for new codes of practice, this is only done on best practice and without statutory underpinning.

The majority of respondents supported the proposal to require the ICO to undertake and publish impact assessments when developing codes of practice and guidance. Respondents acknowledged that this would increase accountability of the ICO which serving as an example of best practice.

To ensure the ICO's codes of practice and significant guidance are effective and useful, the government will take forward the proposal to require the ICO to carry out expert panels, with respondents arguing that the establishment of expert panels would help improve the quality of guidance and increase public trust in the regulator's work. However, proposal, with respondents raising concerns over membership of the expert panels, and the need for transparency in the governance process.

To ensure the ICO's codes of practice and statutory guidance are effective and useful, the government will take forward the proposal to require the ICO to set up expert panels. The ICO's cross-sector regulation, a broad and transparent consultation process will be an expert panel will improve the ICO's understanding of how legislation may apply to different sectors and organisations. The ICO will have the flexibility to determine the composition of the panel, a summary of its findings and a response on how, and to what extent, they have reflected these findings in the code or statutory guidance.

Approval of codes of practice and complex or novel guidance (question 5.5.2)

The government proposed that the requirements to carry out impact assessments and to establish expert panels would also apply to the ICO's codes of practice. The Secretary of State to approve codes of practice and complex or novel guidance.

The majority of respondents disagreed with this proposal. Respondents mainly highlighted concerns about the risk to the ICO's independence.

The government believes that the new requirements on the ICO to carry out impact assessments and to establish expert panels will ensure that the ICO's statutory procedures are more robust. However, the government also believes it is important to demonstrate accountability that such guidance is approved by the DCMS Secretary of State, as it has safeguard for this process, before the guidance is laid in Parliament.

The government therefore intends to proceed with introducing a process for the Secretary of State to approve the ICO's codes of practice and complex or novel guidance, exempt (for example, guidance on ICO internal processes). For transparency, the Secretary of State will be required to publish their reasons for approving or not approving a statutory code or statutory guidance produced by the ICO.

Applying these proposals more broadly (questions 5.5.4, 5.5.5)

The government proposed that the requirements for the ICO to be a broader set of the ICO regulatory products, and whether the ICO should be required to undertake and publish an impact assessment on each and every guidance product.

There were mixed views on whether to extend the proposed requirements on impact assessments and expert panels to all non-statutory guidance. Respondents highlighted the need for a proportionate approach, with some arguing that the impact on ICO independence.

The government will not pursue extending the proposals to all non-statutory guidance and requires an impact assessment on every guidance product. Respondents highlighted the need for a proportionate approach, with some arguing that the impact on ICO independence. The government will not pursue extending the requirements, and will instead limit the scope to all statutory codes of practice and statutory guidance unless exempt.

5.6 Complaints

The current legislation forces the ICO to allocate a significant amount of its resources to handling data protection complaints, yet many such data protection complaints could be resolved more effectively between the complainant and relevant data controller without the involvement of the ICO.

Under the UK GDPR and the DPA 2018, there is currently no threshold to make a complaint to the ICO. Internationally, this contrasts with other regimes such as the Canadian OPC, which requires that individuals should first give the organisation they complain to the Commissioner, also provides guidance outlining when the Commissioner may decide not to investigate a given complaint, including if the complaint is not in the ICO's view reasonable efforts to resolve the complaint directly with the data controller first.

Reform of the complaints framework (questions 5.6.1, 5.6.2, 5.6.3, 5.6.4)

The government will not proposed to create a threshold for a complaint to be made, which would require a complainant to attempt to resolve their complaint directly with the relevant data controller before contacting the ICO. The government will instead recommend or data controllers to have a simple and transparent complaints handling process in place to deal with data subject complaints.

To further enable the ICO to allocate resources efficiently and effectively against the highest data protection risks, the government will proceed with the proposal to introduce a new power for the ICO to be able to cease to investigate a complaint. Concerns were raised that this could lead to data controllers ceasing to cooperate with the ICO can decide not to investigate a given complaint.

Around half of respondents agreed that the ICO would benefit from a more proportionate regulatory approach to data protection complaints. Respondents were keen to highlight some concern over a potential risk of undermining data subject rights. The ICO's ability to cease to investigate a complaint, if it deems it appropriate, contrasts to the ICO's core remits. At the same time, many respondents agreed that a more proportionate approach would be beneficial to the ICO, data controllers and better outcomes and clearer expectations for all parties.

The majority of respondents supported the proposal to require complainants to reach out to the data controller before contacting the ICO. Respondents felt this would lead to better outcomes for data subjects, would reduce the number of complaints and would reduce the volume of 'premature' complaints going to the ICO. Many respondents noted that this proposal also currently reflects best practice, via the ICO's guidance and would not be a change for most. Although there was a small number prior to any further regulatory action.

Around half of respondents agreed with the proposal to set out a criteria in legislation by which the ICO can decide not to investigate a complaint. Concerns were raised that the ICO could be seen as not being independent if it ceased to investigate a complaint.

The vast majority of respondents agreed with introducing a requirement for data controllers to have a simple and transparent complaints handling process to deal with data subjects' complaints, although some respondents stressed that any such requirement should be proportionate and should avoid being burdensome on organisations.

The government intends to proceed with these proposals. The ICO will have the ability to use its discretion to decide when and how to conduct a complaint. The ICO will have clear discretion in legislation not to investigate certain types of data protection complaints, for example, where the complaint is vexatious or where the complainant not first attempted to resolve the issue with the relevant data controller. This will empower the ICO to exercise its discretion with confidence. In turn, data controllers will be able to better understand their responsibilities and data subjects their rights.

The government recognises the concerns raised around the ICO ceasing to investigate proceeding with these proposals will ensure that data subject rights are properly safeguarded. The government will also require data controllers and processors to complain to the ICO if the issue cannot be resolved with the controller.

This new regulatory approach will empower the ICO to take a more agile approach to complaints, in turn allowing its resources to be used in a more risk-based way.

5.7 Enforcement powers

The ICO is responsible for monitoring and enforcing the UK's data protection regime. The ICO should be a strong, effective regulator that is equipped with the powers it needs to ensure compliance with the UK data protection legislation and take action where necessary, when organisations and individuals undertake unlawful personal data processing.

The government explored 3 areas where the ICO's powers may need to be extended in limited circumstances, which focus on enabling the ICO to carry out more effective and efficient enforcement activity. These were:

- Power for the ICO to commission technical reports.
- Power to compel witnesses to attend and answer questions at interview.
- Extending the statutory deadline for the ICO to issue a penalty following a notice of intent.

The majority of respondents supported the proposal to commission technical reports. Respondents felt this would enable the ICO to carry out more effective and efficient enforcement activity. These were:

- Power for the ICO to commission technical reports.
- Power to compel witnesses to attend and answer questions at interview.
- Extending the statutory deadline for the ICO to issue a penalty following a notice of intent.

The majority of respondents supported the proposal to compel witnesses to attend and answer questions.

The government plans to proceed with the power for the ICO to compel witnesses to attend an interview and to compel the witness to answer questions. While there was a small number of respondents who raised concerns that this could be used against Market Authority and Financial Conduct Authority that compel witness, some respondents worked reassurance that appropriate safeguards would prevent this power from being misused by the ICO.

The ICO's new power will not be established in a way which interferes with the rights of individuals not to incriminate themselves. The government recognises the risks of unintended consequences which ensure that witnesses and witness interviews are conducted in a way that is proportionate and lawful.

Amend the statutory deadline for the ICO to issue a penalty following a notice of intent (questions 5.7.1, 5.7.2)

The government proposed to extend the ICO's power to have flexibility on the time available to issue a penalty notice following a Notice of Intent, where needed. Today, however, the current statutory 6-month deadline to 12 months, which the majority of respondents supported. The government proposed to extend the statutory deadline to an unlimited time beyond the 6-month deadline under certain circumstances, which the majority of respondents supported. Respondents who supported these measures felt that it would lead to better, fairer outcomes for data subjects and that these measures were concerned about the reputation of the ICO by stating.

The government plans to proceed with the second of these options, as this will provide the ICO with the flexibility it needs to ensure it can conclude its investigations where it does not extend the deadline across the board.

Enhancing the ICO's transparency regarding investigations (question 5.7.3)

The consultation proposed greater transparency mechanisms by placing a requirement on the ICO to publish its strategy for how it will conduct its investigations and to inform data controller at the beginning of an investigation.

The majority of respondents supported this proposal. Respondents felt that ICO transparency would lead to better outcomes for data subjects and would be a helpful tool. Of those that disagreed, respondents argued that this was an unnecessary process for the regulator.

The government plans to proceed with this proposal in order to provide greater clarity to data controllers since an ICO investigation is underway.

5.8 Biometrics Commissioner and Surveillance Camera Commissioner

The consultation outlined the need to simplify the oversight framework for police use of biometrics and police and local authority use of surveillance cameras. The regulatory landscape is crowded and confusing, which can inhibit innovation and public trust in the use of these technologies. The Biometrics Commissioner and the Surveillance Camera Commissioner and the ICO. This can be particularly confusing where biometric and surveillance technologies converge, for example the use of live facial recognition in public spaces.

The government recently simplified these arrangements by appointing Tony Porter to oversee the Biometrics Commissioner and the Surveillance Camera Commissioner. This has simplified by allocating the functions of these commissioners under one office, with an aim of creating a single hub for advice, guidance and notices for data controllers and the public.

The majority of respondents were supportive of simplification. Of those who agreed, many highlighted the need for a clear and transparent process for the transfer of functions. For example, some respondents highlighted the potential for greater efficiency in dealing with a single body as well as removing areas of overlap, such as similar guidance produced by the ICO and the Surveillance Camera Commissioner.

Some respondents disagreed with the proposal to absorb the functions of the Biometrics and Surveillance Camera Commissioners into the ICO. Some felt that the ICO might become overstretched, given the breadth of its regulatory scope. Others highlighted the importance of the ICO's independence from the Government and political functions of the Biometrics Commissioner, who reviews applications from the police to retain biometrics in very limited circumstances when people have not been convicted.

In light of this feedback and wider engagement, including with the current Biometrics and Surveillance Camera Commissioners, the government has decided that it will not take forward the proposal to simplify the oversight framework in this area.

The Biometrics Commissioner's oversight functions provide important independent oversight, particularly in relation to national security. Redefining the feedback from the Biometrics and Forensics Ethics Advisory Committee (BFEAC) and the ICO. The functions are all considerable transferring these functions to the Investigatory Powers Commissioner, acknowledging the relevant expertise that they provide in relation to national security.

Independent oversight of the use of surveillance technology is also considered to maintain public trust. The Surveillance Camera Commissioner provides independent oversight of the use of CCTV and ANPR systems by police and local authorities. It oversees the use of these technologies by others. This duplicates the relationship between respondents in the consultation, particularly in relation to guidance issued by both the Surveillance Camera Commissioner and the ICO. The government believes that this need clear and consistent guidance to be in place and that the Surveillance Camera Commissioner and therefore plans to simplify oversight by removing this duplication.

The government recognises the importance of the Surveillance Camera Commissioner's role in providing independent oversight of the use of surveillance technology in public spaces. The government believes that the ICO is better placed to provide this oversight, particularly given the ICO's independence from the Government and political functions of the Surveillance Camera Commissioner. The government therefore intends to proceed with transferring the Surveillance Camera Commissioner's functions to the ICO.

Sector Organisations (SO) and Statutory Consumer Protection Bodies (CPB), such as the Pharmacy Inspectorate of Consultancy and Fee & Rescue Services and the College of Policing also have the ability to play a larger role.

5.9 Further questions

At the end of this chapter, the Council seeks views on whether any of the proposals would impact on anyone with protected characteristics. There were no specific proposals that we believe would disproportionately affect those with protected characteristics, we were there significant issues raised by respondents in relation to the questions and topics in this chapter.

The consultation also posed some open-ended questions at the end of this chapter for respondents to provide any other comments on the proposed reforms. Respondents raised several issues that were outside the scope of this consultation, but which we will take into account when considering the wider operational implications. The protection of people's personal data is already at the heart of the UK's data regime and will continue to be so as the government embarks on its reform agenda.

Questions on analysis of expected impact

The consultation was published alongside a suite that contained the second assessment to measure the expected impact of the proposed policy proposals. In this note, we outlined our methodologies, some initial results and also the areas we believed were most sensitive and that could be gained from the consultation stage for the final impact assessment.

Respondents were asked a series of questions surrounding the compliance activities that they currently undertake under the current regime, how much they estimate they currently cost them and how they believed these would change if the reforms were implemented. The responses to these questions would help us to better understand how UK business compliance activities and strengthening the evidence base of our impact assessment.

The consultation responses indicate that the stakeholders that responded to these questions are largely content with the analysis estimates so far. This includes the methodological approach and sources of costs and benefits of these reforms. What it also highlights is that there is a wide range of costs that could be affected and be applied. This has allowed us to further evidence our modelling and analytical methodology by conducting a sensitivity analysis on the results and further taking into consideration the wider impacts of the reforms. We have also considered the potential diversity between firms affected and reflect the inherent uncertainty on impacts that respondents indicated to us. We will ensure these are incorporated in the final impact assessment.

Over half of all respondents to these questions carry out all of the compliance activities listed in our analysis. The vast majority of these respondents highlighted that they spend the most time and resources on personal data processing and cookies compliance. Many also noted that they spend a significant amount of time and time responding to subject access requests, preparing data protection impact assessments and maintaining ROPA. The consultation also highlighted that the changes to these processes will vary in impact.

Responses on the current cost of these activities for UK businesses varied, the consensus being that for smaller businesses and core traders it is harder to calculate these costs. Often it forms only a proportion of a full time equivalent worker's (FTE) or time of a senior manager/director and is not a separate cost centre. There is also a number of firms that highlighted that although some compliance activities are core to time, they are used beneficial when creating a framework and can lead to cost savings in the long run.

Respondents had a mixture of opinions on how the proposed reforms may impact the compliance costs they currently face. Many respondents highlighted the potential increase in compliance costs for activities surrounding data subject access requests, personal data and responding to subject access requests. However, many other respondents were also concerned that whilst there may by benefits, there would also be transition costs to adapt to the new regime. Many also noted that they were further concerns around the impacts to consumer confidence in using a business and the impact these reforms may have on international relations. Of all of the activities listed in our analysis, respondents highlighted that the impact on the cookies activities were most likely to be impacted by the proposed reforms.

In terms of international transfers, the majority of respondents either rely on EU adequacy or the use of Standard Contractual Clauses (SCC) to transfer personal data across borders, and welcome a set of reforms that make the use of these transfer mechanisms easier. The consultation also highlighted that the use of these mechanisms is the risk of a change in the UK's current adequacy status and the impact on businesses if adequacy were to be lost.

The consultation also asked for views on the assessment which will include updated analysis of the expected impact of the proposals. Following the policy changes made in light of the responses we have received, as well as the updates we have made to our analysis, we will publish an updated IA ahead of the reforms coming into the analysis that was published alongside the consultation.

Public sector equality duty analysis

The government has given due consideration to the public sector equality duty, under the Equality Act 2010, and the consultation exercise was especially undertaken in relation to the following areas:

Subject access requests. Our pre-consultation analysis considered whether the re introduction of a nominal fee for subject access requests could impact on disadvantage individuals who make these requests, and this was highlighted in a number of responses to the consultation. Subject access requests are used by individuals with protected characteristics, particularly age and disability. The government will not re introduce a nominal fee for subject access requests and will instead consider other measures to deter the vexatious requesters, whilst ensuring whether enhancing a better safeguard in the Data Protection Act 2018 as the provided under Section 78 of the Freedom of Information Act (for public bodies) to deter vexatious requesters. The government believes that the Information Commissioner deserves the current duty to facilitate data subject rights under Article 12(2) GDPR and Section 52(2) of the DPA 2018 to be sufficient. Potential revised guidance from the ICO could be helpful in providing further clarity on what is considered vexatious. The government is satisfied that proposals in the consultation are not disproportionately impact groups with protected characteristics.

Legitimate interests. Our pre-consultation analysis noted the potential indirect impact on those with protected characteristics who are disproportionate characteristics. This was supported by respondents, who warned that removal of the requirement to take individuals' rights and interests into account in a wide range of circumstances could have a disproportionate impact on certain vulnerable groups in society, who are less able to complain to the regulator if their personal data has been misused. Having considered consultation responses, the government has decided not to proceed with the proposal to remove the requirement to take individuals' rights and interests into account when using legitimate interests as a lawful basis. This could include, for example, processing that is necessary for crime prevention or IT security purposes, or for employee monitoring or for direct marketing purposes. In these situations it could encourage organisations to make the authorities aware of individuals who are at risk, without delay. This could have direct benefits for children and other vulnerable individuals who are victims of crime, or who are at risk of being removed in these scenarios. Jobs controllers would continue to be required to conduct a balancing test, and to document their assessment (to ensure accountability and transparency), which would further reduce the risks of any adverse impact on groups with protected characteristics.

Cookie proposals. Some respondents raised concerns about websites processing increased volumes of personal data without consent, especially where the data processing is undertaken by third parties. Some respondents also noted that they felt nobody knew enough about the importance of and understanding the user appropriate design codes (AADC) standards, notably the need for a high level of transparency and protection for children's data online. The ICO and the government will take forward it, permitting audience measurement and volume measurement cookies to be placed on a website without consent, but with adequate safeguards to protect the rights of individuals, such as limiting any information that is collected about individuals, not using the information to make decisions about individuals, and not using the data for more intrusive purposes. A lower fine of up to 4 or out-of-current model for websites would only take place once ministers are satisfied that the ICO has sufficient powers and resources in place to effectively manage their performance on how their data is processed.

Extending the soft opt-in to non-commercial organisations (such as political parties). Our pre-consultation analysis noted that the proposal to extend the soft opt-in would mean that some people will receive direct marketing messages that they would not have received before, which could be a nuisance to them. Some groups with protected characteristics (such as mental health issues) may be more concerned than others by details, for example, of political parties' views on issues. The ICO's Direct Marketing Guidance, which the government will design the proposal on, that non-commercial organisations are subject to exactly the same rules as commercial organisations in terms of respecting a person's right to opt-out and maintaining a record for them to do so.

ICO complaints. Concerns were raised by some respondents that requiring data subjects to complain to the relevant controller before complaining to the ICO would disadvantage those with protected characteristics, who may be less confident or less able to exercise their rights to complain or seek redress. To mitigate these risks, we will consider the proposals with sector-specific colleagues. As such, the data subject will continue to be able to complain to the ICO, and the ICO will be required to send an adequate response after a set time period, if the controller has not responded. The ICO will also be able to take action against controllers who breach data subject rights, and also retain current statutory accountability mechanisms to ensure that the ICO is accountable for its decisions and complaint handling processes. Under Article 12(2) GDPR controllers the right of subject entirely where the supervisory authority does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint", and this will be maintained.

AI proposals. In our pre-consultation analysis we considered how our proposal on creating a new condition for processing of sensitive personal data for bias monitoring purposes in AI systems, could impact on those with protected sector equality duty under section 149(1) Equality Act 2010. This proposal is likely to lead to more organisations being able to process personal data relating to protected characteristics. The purpose of the proposal is to support organisations to monitor and correct bias in AI systems, and to ensure that decision-making systems are consistent/unbiased so that they. Furthermore, the more representative the data that an AI system is trained on, the more the system will reflect a broader cross section of society, and the less likely it is to perpetuate existing bias, discrimination, or an individual with protected characteristics. Similar considerations were involved in a closely related proposal for processing of personal data for bias and error monitoring in relation to AI systems. Organisations would not be required to take individuals' rights and interests into account when relying on the "legitimate interests" ground to process personal data for bias and error monitoring purposes, if certain safeguards are in place and met. The proposal attempts to legitimate interests outlined above in the paragraph on legitimate interests.

Future-proofing Article 22. Consultation responses raised concerns over the proposal to remove the requirement for organisations to consider the right to human review could have a disproportionately negative impact on people with protected characteristics, for example on the basis of their sex or race. A frequently cited example was AI used in recruitment, which could lead to a discriminatory, fail discriminated unfairly against people. Through precautions were taken to prevent bias based on protected characteristics, the profiles of those attending different universities could be biased against people with protected characteristics, including race and sex. In this example, there was unanything over the appeal mechanisms pupils could access. Our proposals retain human review as a safeguard in Article 22 UK GDPR, but remove the requirement for organisations to cause safeguards for any significant decision made without meaningful human involvement, potentially to include a justification of how a decision is reached which could be challenged. We have clearly identifying how protected characteristics have been factored into a decision.

Removal of prescriptive requirements to complete data protection impact assessments (DPIAs). Our pre-consultation analysis considered whether this proposal could have a disproportionate impact on those with protected characteristics. The processing for individuals with protected characteristics is not identified. However, organisations will still be required to consider risk through implementation of their data protection management programmes and DPIAs remain a tool that could help mitigate the potential risk of protected characteristics not being identified.

Overall, our analysis is still that the government does not consider that any negative impact of our proposals on individuals with protected characteristics are disproportionate.

Annex A: List of consultation proposals

Question	Proposal	Next steps
1.2.1	Consultation/research processes into a single chapter	6: The government plans to proceed with this proposal
1.2.2	Creating a statutory definition of scientific research	6: The government plans to proceed with this proposal
1.2.8	Incorporating broad consent for scientific research into legislation	6: The government plans to proceed with this proposal
1.2.9, 1.2.10	Creating a new lawful ground for processing for research purposes	C: The government does not plan to proceed with this proposal
1.2.15	Clarifying that further processing for an incompatible purpose may be lawful where based on a law that safeguards an important public interest, or where the data subject has consented	6: The government is considering this proposal further
1.2.23	Clarifying when further processing can be undertaken by a controller different to the original controller	6: The government is considering this proposal further
1.2.24	Clarifying when further processing may occur in the context of a lawful ground and consent	6: The government plans to proceed with this proposal
1.2.30	Extending the "disproportionate effort" exemption an information provision obligation to organisations processing for research purposes of personal data collected directly from the data subject	6: The government plans to proceed with this proposal
1.4.1, 1.4.2, 1.4.4	Creating a limited set of legitimate interests for businesses to process personal data without applying the balancing test	6: The government plans to proceed with this proposal, with a narrower set of legitimate interests than set out in the consultation
1.4.3	Including process necessary for the purpose of ensuring bias monitoring, detection and correction in AI systems in the legitimate interests, if proposed be created under 1.4	C: This will not be included in the narrow list of legitimate interests, the balancing test is not required.
1.5.11, 1.5.12, 1.5.13	Enable organisations to use sensitive personal data for the purpose of managing bias in AI systems, by creating a condition that Schedule 1 Paragraph 8 can be used for processing necessary for the purpose of ensuring bias monitoring, detection and correction	6: The government plans to proceed with this proposal
1.5.23	Developing a safe regulatory space for the development, testing and training of AI	C: The government does not plan to proceed with this proposal
1.5.1, 1.5.2	Addressing uncertainty about the scope & substance of fairness in the DP regime is applied to the development, deployment and use of AI systems and the ICO's regulatory remit	6: The government is considering this proposal further
1.5.14, 1.5.15, 1.5.16, 1.5.17	Clarifying the limits and scope of Article 22 UK GDPR	6: The government plans to proceed with this proposal
1.5.17	To remove Article 22 of UK GDPR and safeguard automated decision making permitted where authorised by law (for example under Schedule 4 Article 9 (2) (g) supplemented by Schedule 1 to the Data Protection Act 2018) where the processing does not involve special category data, rest of the data protection regulation	C: The government does not plan to proceed with this proposal
1.6.1, 1.6.2	Adapting the Council of Europe's test for anonymisation into legislation	6: The government plans to proceed with this proposal
1.6.3	Confirming that the test for anonymisation is a relative one	6: The government plans to proceed with this proposal
2.2.12	Raising the threshold for when data breaches are notifiable to the ICO under Article 33(1) of the UK GDPR	C: The government does not plan to proceed with this proposal
2.2.2, 2.2.3, 2.2.4, 2.2.5	Require organisations to operate a privacy management programme	6: The government plans to proceed with this proposal
2.2.5, 2.2.6, 2.2.7	Replace the requirement to appoint a DPO with a requirement to designate a suitable individual to oversee the organisation's DP compliance	6: The government plans to proceed with this proposal
2.2.8	Remove the requirement to Data Protection Impact Assessments	6: The government plans to proceed with this proposal
2.2.9	Remove the requirement to Prior Consultation with the ICO on high risk processing	6: The government plans to proceed with this proposal
2.2.10	Introduce a new "voluntary undertakings" process	C: The government does not plan to proceed with this proposal
2.3.3	Introducing a cost ceiling for complying with subject access requests	6: The government plans to proceed with this proposal
2.3.1, 2.3.2, 2.3.3	To amend the threshold for refusing to comply with subject access requests to "manifestly unfounded or excessive" to "excessive" or "manifestly unfounded"	6: The government plans to proceed with this proposal
2.3.4	Introducing a nominal fee for subject access requests	C: The government does not plan to proceed with this proposal
2.4.4	To remove the requirement for prior consent for certain cookies (those falling outside the requirements of Regulation 6 of PECR)	6: The government plans to proceed with this proposal, but will explore how to make cookie consent easier for users to manage online preferences
2.4.1	To remove the consent requirement for Regulation 6 of PECR for a wider range of purposes than just those currently exempt (exempting Regulation 6 of PECR for "small audience" cookies)	6: The government plans to proceed with this proposal
2.4.3	To remove the consent requirements in Regulation 6 of PECR for a wider range of purposes than just those currently exempt, demonstrable legitimate interest for processing	6: The government plans to proceed with this proposal
2.4.2	To remove the consent requirements in Regulation 6 of PECR where controllers are able to demonstrate legitimate interest compliance with a UK-equivalent version of code or regulatory guidance	6: The government plans to proceed with this proposal
2.5.2	Exempting business-to-business electronic communications from PECR's opt-in direct marketing by electronic means	C: The government does not plan to proceed with this proposal
2.5.8	Extending the soft opt-in for direct marketing to communications from political parties	6: The government plans to proceed with this proposal
2.5.3	Extending the soft opt-in for direct marketing to communications from charities (registered and registered/with the Electoral Commission) third-party campaign groups	6: The government plans to proceed with this proposal
2.4.9	Extending the soft opt-in for direct marketing to communications from political parties and commercial organisations	6: The government plans to proceed with this proposal
2.4.10	Empowering ICO to take action against organisations for the number of unsolicited marketing messages sent, if as well as calls "received and connected"	6: The government plans to proceed with this proposal
2.4.11	Introducing a 'duty to report' on communication service providers to report suspicious traffic branding their networks	6: The government plans to proceed with this proposal
2.4.12	Limited time period for unsolicited marketing calls	6: The government is considering this proposal further
2.4.13	Requiring communications providers to do more to block calls / texts of course	6: The government is considering this proposal further
2.4.13	Mandating communications providers to automatically block calls from numbers for incoming calls not on an allow list	6: The government is considering this proposal further
2.4.13	Empowering ICO to impose assessment notices on communications suspected of PECR breaches	6: The government plans to proceed with this proposal
2.4.14	Requiring websites to respect preferences set by individuals through their browser	6: The government plans to proceed with this proposal
2.4.16	Increasing fines under PECR to GDPR levels	6: The government plans to proceed with this proposal
2.4.16	Other measures to help ensure the enforcement regime is effective, proportionate and dissuasive	6: The government plans to proceed with this proposal
3.3.7	To reform the DCMS Secretary of State's adequacy making power	6: The government plans to proceed with this proposal
3.3.2	Making adequacy regulations for groups of countries, regions and multilateral frameworks	6: The government will continue to consider this approach
3.3.3	To remove the requirement for the DCMS Secretary of State to conduct a review of adequacy decisions every 4 years	6: The government plans to proceed with this proposal
3.3.7	Clarifying that either judicial or administrative redress is acceptable for international transfers	6: The government plans to proceed with this proposal
3.3.3	Exempt "reverse transfers" from the scope of the UK GDPR	C: The government does not plan to proceed with this proposal
3.3.4	Empowering organisations to create their own IDTAs	C: The government does not plan to proceed with this proposal
3.3.5	Creating a new power for the DCMS Secretary of State to formally recognise new IDTAs	6: The government plans to proceed with this proposal
3.3.5	Reinforcing the importance of proportionality when using IDTAs	6: The government plans to proceed with this proposal
3.4.1	Allowing certification for international transfers, to facilitate innovative approaches to accountability	C: The government does not plan to proceed with this proposal
3.4.1	Clarifying that prospective certification schemes can be used as a transfer mechanism (as UK-approved international transfer schemes	C: The government does not plan to proceed with this proposal
3.5.1	Establishing a proportionate increase in flexibility for use of derogations by making "occasionally" and "not to be repetitive" in permitted	C: The government does not plan to proceed with this proposal
4.2.1, 4.2.2, 4.2.3	Clarifying that organisations acted to carry out an activity on behalf of a public body in the public interest, should be considered controllers rather than processing the personal data under Art 6(1)(e)	6: The government plans to proceed with this proposal
4.2.1	To extend powers under section 32 of the Charities Act 2011 to permit charities to share public service delivery to business undertakings, beyond the current scope of solely individuals and households	6: The government plans to proceed with this proposal
4.4.5, 4.4.6, 4.4.7	Defining "substantial public interest"	C: The government does not plan to proceed with this proposal
4.4.7	Specifying new situations in sch 1 DPA 2018 where data may be processed on grounds of substantial public interest	6: The government plans to proceed with this proposal
4.2.3	Clarifying that health data can be lawfully processed when necessary for research substantial public interest in a public health context, and for research and oversight by healthcare professionals	C: The government does not plan to proceed with this proposal
4.4.8	Clarifying rules on the collection, use and retention of biometric data by the police	6: The government plans to proceed with this proposal
4.5.1	Align key terms that are used across the different data processing frameworks for greater consistency	6: The government plans to proceed with this proposal
4.6.1, 4.6.2, 4.6.3	Introducing compulsory transparency reporting providing information on how public sector organisations procure and deploy automated tools to support decision-making	6: The government does not plan to proceed with this proposal
5.2.1	New statutory framework setting out the ICO's strategic objectives and duties	6: The government plans to proceed with this proposal
5.2.2	A new oversight duty for the ICO to actively data rights and to encourage foundational and responsible data use	6: The government plans to proceed with this proposal
5.2.4	New duty for the ICO to have regard to economic growth and innovation	6: The government plans to proceed with this proposal
5.2.5	New duty for the ICO to have regard to competition issues	6: The government plans to proceed with this proposal
5.2.6, 5.2.7	New duties for the ICO to consult with relevant bodies and to have regard to their views when exercising its duties to have regard to growth, innovation and competition	6: The government plans to proceed with this proposal
5.2.8	Establish a new information sharing gateway to support regulatory cooperation	C: The government does not plan to proceed with this proposal
5.2.10	Requirement for the ICO to deliver a more transparent and structured international strategy	C: The government does not plan to proceed with this proposal
5.2.10	New statutory objective for ICO to consider wider IPRO international priorities	6: The government plans to proceed with this proposal
5.2.10	New duty for the ICO to have regard to public safety	6: The government plans to proceed with this proposal
5.2.11	New power for the DCMS SoS to prepare a statement of strategic priorities which the ICO must take account of	6: The government plans to proceed with this proposal
5.3.1	Establish as independent Board and Chief Executive for the ICO	6: The government plans to proceed with this proposal
5.3.2	Appointing the Chair by the same process as that for appointing the C under DPA 2018	6: The government plans to proceed with this proposal
5.3.3	Appointing the non-executive board members by the DCMS SoS	6: The government plans to proceed with this proposal
5.3.4	Chief Executive to be appointed by the DCMS Secretary of State, following a fair and open	6: The government does not plan to proceed with this proposal

	Secretary of State. Alternative recommendation is for this to be an ICO Board appointment, in consultation with the DCMS Secretary of State.	not plan to proceed with this proposal
5.4.1	Removing Parliamentary approval to amend IC's salary	A - The government plans to proceed with this proposal
5.4.2	Requirement for the ICO to develop & publish KPIs	A - The government plans to proceed with this proposal
5.4.3	Requirement for the ICO to publish key strategies and processes guiding its work	A - The government plans to proceed with this proposal
5.4.3	Requirement for ICO to publish other information to aid transparency	A - The government plans to proceed with this proposal
5.4.6	A power for the DCMS Secretary of State to initiate an independent review of the ICO's activities and performance	C - The government does not plan to proceed with this proposal
5.5.3	A process for the DCMS Secretary of State to approve statutory codes of practice and statutory guidance ahead of laying them in Parliament	The government plans to proceed with this proposal
5.5.1	A power for the DCMS Secretary of State to require the ICO to set up a panel of experts when developing all codes of practice and statutory guidance, unless exempt	A - The government plans to proceed with this proposal
5.5.2	To require the ICO to undertake and publish impact assessments when developing all codes of practice and statutory guidance unless exempt	A - The government plans to proceed with this proposal
5.6.2, 5.6.3	Requiring data controllers to have complaints-handling mechanisms	A - The government plans to proceed with this proposal
5.6.2, 5.6.3, 5.6.4	Set out in legislation the criteria 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.	A - The government plans to proceed with this proposal
5.7.2, 5.7.3, 5.7.4	New power to commission a technical report to aid breach investigations	A - The government plans to proceed with this proposal
5.7.7	Changing statutory deadline for ICO to issue a penalty from 6 to 12 months	C - The government does not plan to proceed with this proposal
5.7.8	Introducing a provision to permit the ICO additional time beyond the 6-month statutory deadline to issue a penalty, under certain circumstances.	A - The government plans to proceed with this proposal
5.7.9	Introducing a requirement for 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.	A - The government plans to proceed with this proposal
5.7.6	New power for the ICO to compel witnesses to interview during investigations and answer questions	A - The government plans to proceed with this proposal
5.8.1, 5.8.2	Further simplification of the oversight framework for the police use of biometrics and overt surveillance	A - The government plans to proceed with this proposal

Annex B: List of organisations that responded to the consultation

- Advertising Association
- Aberdeen City Council
- abrdn plc
- ABUKAI
- Access Now (NGO working for the protection of human rights in the digital age)
- Action Medical Research
- ActionAid UK
- Ada Lovelace Institute
- ADR UK
- ADS Group
- Airbus
- Airbus Operations Limited
- Akrivia Health
- Alan Turing Institute
- Alternative Investment Management Association (AIMA) and the Alternative Credit Council (ACC)
- Alzheimer's Society
- Amberhawk Training Limited
- Anekanta Consulting
- Aneurin Bevan University Health Board (NHS Wales for Gwent)
- Anthony Nolan
- AOP - Association of Online Publishers
- APIMS Limited
- AQA
- Arc Data Limited
- Archives and Records Association
- Ardonagh Advisory
- ARTICLE 19
- Association for Interactive Media and Micropayments
- Association of British HealthTech Industries
- Association of British Insurers
- Association of Medical Research Charities (AMRC)
- AstraZeneca
- ATI
- Audit Wales
- Avast Software
- Awin
- Azorus
- BACP
- BAE Systems Applied Intelligence Limited (ICO registration number: Z5470019)
- Bail for Immigration Detainees
- Battersea Cats and Dogs Home
- Baycloud Systems
- BCP COUNCIL
- BCS - The Chartered Institute for IT
- Behold.ai Technologies Limited
- Best Companies Limited
- Betting and Gaming Council
- Big Brother Watch
- BILETA
- Biotechnology Innovation Organisation
- Birmingham University
- Bolton Council
- BongoIT
- BPE Solicitors LLP
- Breakthrough Communications and Strategies Limited
- Breast Cancer Now
- Bird & Bird LLP
- British American Business
- British and Foreign Bible Society
- British and Irish Law, Education and Technology Association (BILETA)
- British Heart Foundation
- British Irish Chamber of Commerce
- British Medical Association
- British Red Cross
- British Retail Consortium
- British Security Industry Association (BSIA)
- BSA
- BSI Group
- BT Group
- Buckinghamshire Council
- CACI UK
- Caerphilly County Borough Council
- Cancer Research UK
- Capita
- Capsticks solicitors llp
- Cardiff University
- Catalyst Housing Limited
- CEDPO
- Center for AI and Digital Policy
- Center for Data Innovation
- Centre for Digital Trust and Society
- Centre for Intellectual Property and Information Law (CIPIL)
- Centrica plc
- Cerner
- CGI
- Chartered Institute of Fundraising
- Cheshire West and Chester Council
- Chichester College Group
- Child Poverty Action Group
- Children 1st
- Children's Hearings Scotland
- Church of England
- Cielo
- Cifas
- CIPL
- Citizens Advice
- City of Edinburgh Council
- City of London Law Society.
- Clarion
- Clean Up Gambling
- CloudPay
- Code Poets Limited
- Colchester Borough Council
- Colleges Scotland
- Collingwood Insurance Company Ltd
- Collinson
- Confederation of British Industry
- Connected Places Catapult
- Consumer Credit Trade Association
- Consumer Data Research Centre and Leeds Institute for Data Analytics, University of Leeds
- Consumer Markets Authority
- Cornwall Council
- Coventry City Council
- Crafted Media
- Creative Privacy Ltd
- Credit Services Association
- CREST
- CREST International
- Crisp
- Croud Inc Ltd.
- CrowdStrike, Inc.
- Curve OS Ltd
- CVG Solutions Ltd
- Data Improvement Across Government
- Data Management Association (DAMA)
- Data Marketing Association (DMA)
- Data Privacy Advisory Service
- Data Protection Education Ltd
- Data Protection Network
- Data Trusts Initiative
- Data, Tech and Black Communities
- De Montfort University
- Debt Recovery Plus Ltd
- defenddigitalme (children's privacy group)
- Dementia UK
- Demondude Ltd
- Demos
- DENBIGHSHIRE COUNTY COUNCIL
- Department for Education, UK Gov
- Department of Finance (NI)
- Department of Health NI
- Derbyshire County Council
- Devon and Somerset Fire and Rescue Service
- Devon County Council
- DFN UK
- DIFC Authority
- DIFC Authority - Commissioner of Data Protection
- Digital Europe
- Digital Health & Care Wales
- Direct Line Group
- Discover Learning Trust
- DMG Media
- Donr
- Dorothy House Hospice Care
- Dorset & Wiltshire Fire and Rescue Service
- Dun & Bradstreet
- Dyfed Powys Police
- E.ON
- East Riding of Yorkshire Council
- EasyJet
- EFL Trust
- Eisai Europe Limited
- Element
- Elzware Ltd
- EPUT
- ESOMAR
- Essex County Council
- Ethicall
- Euro parking Services Ltd
- European Centre for Digital Rights
- European Publishers Council
- evalian
- Evergreen Finance London Ltd
- Experian
- Fable Data
- Facewatch Ltd
- Faculty of Actuaries
- Faculty of Advocates
- Faegre Drinker Biddle & Reath LLP
- Fair Trials
- Farrer & Co LLP
- Federation of Small Businesses
- Finance and Leasing Association
- Financial Conduct Authority
- For Your Information
- Forbes Solicitors LLP
- Fundraising Regulator
- Future Plc
- Garmin (Europe) Limited
- GBG PLC
- GDPR In Schools Limited
- GDS Analytics Limited
- Gemserv
- Gener8
- General Council of the Bar
- General Medical Council
- Glasgow Kelvin College
- Global Cyber Alliance
- Global Data Alliance
- Global Privacy Alliance
- Google
- GP Practices
- Great Ormond Street Hospital
- Great Western Air Ambulance
- Greater Manchester Combined Authority and Transport for Greater Manchester
- GreenNet Ltd
- GSK
- Hammersmith & Fulham Council
- Hampshire and Isle of Wight Fire and Rescue Service
- HD Media CIC
- Healios
- Health Data Research UK
- Health Research Authority
- Health Shield friendly Society
- HelloDPO Ltd
- Help for Heroes
- Heriot-Watt University
- Hermes Parcelnet Ltd
- Higher Education Statistics Agency
- Historic Environment Scotland
- HIWFRS
- HM Revenue and Customs
- Hogan Lovells International LLP
- HQBS Ltd
- Huawei Technologies (UK) CO.,Ltd
- HY Education Solicitors Limited
- Hymans Robertson LLP
- ICAEW
- ICO
- IGfL - Information Governance for London
- ILF Scotland
- Immuta
- Impellam Group plc
- Imperial College London
- Independent Healthcare Providers Network
- Information Accountability Foundation
- Information and Records Management Society.
- Information Governance for London
- Information Governance, Betsi Cadwaladr University Health Board
- Information Technology Industry Council (ITI)
- Innoscite Limited
- Inside Futbol Ltd
- Institute of Development Professionals in Education (IDPE)
- Institute of Economic Affairs
- Interactive Advertising Bureau
- International Committee of the Red Cross
- International Regulatory Strategy Group (IRSG)
- Internet Association
- Investment & Life Assurance Group
- Ionx Solutions
- IPRS Group Ltd
- Ipsos MORI
- IQVIA
- ISACA
- ISBA
- ITN
- ITV
- iVIEW
- Japan Christian Link
- Jisc
- JP Legal Assist Limited
- Judicium
- Just Algorithms Action Group
- Keep Our NHS Public
- King Edward VI School
- King's College Hospital Charity
- KIng's College London
- Kingston University
- Lane, Clark and Peacock
- LAUDIS Business Advisors
- Law Society of England and Wales
- Law Society of Scotland
- Lawyers in local government
- Liberal Democrats
- Liberty
- LimApp Ltd
- Lincolnshire Partnership NHS Foundation Trust
- Linklaters LLP
- Local Government Association
- Leicester, Leicestershire and Rutland Local Medical Committee
- London and International Insurance Brokers Association
- London Borough of Barnet
- London Borough of Hounslow
- London School of Economics
- London Stock Exchange Group
- London Strategic Information Governance Networks' Forum
- Londonwide Local Medical Committees
- Look Ltd
- Lowell Financial Ltd
- LSE Law School
- Macmillan Cancer Support
- Marie Curie UK
- Market Research Society
- Mastercard
- medConfidential
- Medical Justice
- Medical Research Council
- Medtronic plc
- MeiraGTx
- Meta
- Methods Analytics
- Microsoft
- Midland Heart Housing Association
- Migrants' Rights Network
- Mind (mental health charity)
- Moorfield Eye Hospital
- More Partnership
- Morgan Sindall Property Services
- Mozilla
- MSite
- Multidimensional Analytics Solutions Ltd
- Munich Reinsurance
- My Data Protection World
- Mydex Community Interest Company
- mySociety
- National Consumer Federation
- National Data Guardian
- National Deaf Children's Society
- National Fire Chiefs' Council (NFCC) Information Governance Group
- National Galleries of Scotland
- National Highways
- National Institute for Care Excellence (NICE)
- National Library of Scotland
- National Physical Laboratory
- National Police Chiefs Council
- Natural History Museum
- NCC Group
- NEC Software Solutions Limited
- New College Durham
- Newcastle City Council
- News Media Association
- News UK
- Newsquest Media Group Limited
- NHS Blood and Transplant
- NHS Business Services Authority
- NHS Confederation
- NHS London Shared Service
- NHS Scotland's Information Governance Forum
- NILGOSC
- Norfolk County Council
- North and Mid Wales Local Authority Data Protection Officers Group
- North Wales Police
- Northdoor plc
- Northern Ireland General Practice Committee
- Northumbria University
- Northumbrian Water Ltd
- noyb - European Center for Digital Rights
- NPCC
- Nuffield Council on Bioethics
- Nuffield Health
- Office for Nuclear Regulation
- One West (part of Bath & North East Somerset Council)
- Onfindo
- Open Data Institute (ODI)
- openDemocracy
- Open Rights Group
- Open University
- Opendium
- Orrick, Herrington and Sutcliffe (UK) LLP
- Oxfam GB
- Oxford University
- Pact
- Paddock Wood Community Advice Centre
- Paper Frogs Ltd
- Parity Technologies, Inc.
- Parking Control Management (UK) Ltd
- Parkingeye
- PCC
- PDSA
- Personal Investment Management and Financial Advice Association (PIMFA)
- Personify XP
- Perth and Kinross Council
- Peterborough City Council and Cambridgeshire County Council
- Peterlee Town Council
- PHG Foundation
- Phillips 66 Limited
- Plaid Financial Ltd
- PomVom UK Ltd
- Pool Data Foundation
- Portsmouth City Council
- Premier Park Ltd
- PreterLex Ltd.
- PrimeConduct Limited
- Prisons and Probation Ombudsman
- Pritchetts Law LLP
- Privacy and Consumer Advisory Group
- Privacy International
- Privacy Partnership
- PrivDash
- Professional Publishers Association
- Public CCTV Managers Association
- Public Law Project
- Racial Justice Network
- RAF Association
- Re:Cognition Health Limited
- REaD Group Ltd
- Redkite innovations
- Reed Global
- Refugee Trauma Initiative
- RELX
- REPHRAIN
- Reply Limited
- Reset
- Revoke Limited
- RGDP LLP
- Ripon Spa surgery
- Royal & Sun Alliance Limited
- Royal and Sun Alliance Limited
- Royal Botanic Garden Edinburgh
- Royal Holloway University
- Royal Mail
- Royal Statistical Society

- Royal Yachting Association
- RSPCA
- Russell Group
- Sage
- Salesforce UK & Ireland
- Salford CVS and the Greater Manchester VCSE Information Governance Lead Group
- Salvation Army
- SAS Software UK
- Sasa Marketing Ltd
- SAT-7 UK
- Save the Children
- Scottish Chambers of Commerce
- Scottish Fire and Rescue Service
- Scottish Government
- Scottish Water
- Siccar
- Sight Scotland and Sight Scotland Veterans
- Skills Development Scotland
- Sky
- Smart DCC Ltd
- Snapchat
- Software & Information Industry Association
- Software and Information Industry Association
- Soha Housing Ltd
- Solutionlabs Ltd
- South East Open Source Solutions Ltd.
- South Somerset District Council
- Specsavers Optical Group
- Sphere Data Protection
- St Albans City and District Council
- Staffordshire County Council
- STAMMA
- Statewatch
- Station10
- Stewardship
- StopWatch
- Strategic Communications (U.K.) ltd
- STREETINVEST
- Sue Ryder
- Surrey MAISP Action Group
- Takeback Software Ltd
- TechUK
- Telford & Wrekin Council
- Tendring District Council
- Terrafirma IDC Ltd
- Tesco Mobile
- Tewkesbury Borough Council
- Thales UK
- Thames Water
- The 3 Million
- The Age Verification Providers Association
- The Alternative Investment Management Association and the Alternative Credit Council
- The Association of British Investigators
- The Association of the British Pharmaceutical Industry
- The British Library
- The Chartered Institute of Fundraising
- The Chartered Institute of Marketing
- The Citizens
- The Coalition for a Digital Economy
- The Common Framework
- The Council for Advancement and Support of Education (CASE)
- The DPO Centre
- The Electoral Commission
- The International Parking Community
- The Joint Council for the Welfare of Immigrants (JCWI)
- The Kubernesis Partnership LLP
- The Law Society of England and Wales
- The Legal Education Foundation
- The Purbeck School
- The Royal Society
- The Salvation Army
- The Scottish Children's Reporter Administration
- The Scouts
- The Southern Co-Operative
- The University of Bradford
- The University of Manchester
- The University of Sheffield
- The Vale of Glamorgan Council
- The Wrekin Housing Group Limited
- Thurrock Council
- TIGA
- TISA (The Investing and Saving Alliance)
- Tony Blair Institute for Global Change
- TRACE Enforcement Group
- Trades Union Congress (TUC)
- TransUnion
- trueCall Ltd
- Trunomi
- Trusthogen.com
- UDL Intellectual Property
- UK Car Park Management
- UK Citizens
- UK Ethics Pandemics Accelerator
- UK Interactive Entertainment (Ukie)
- UK Online Measurement Company
- UKAS
- UKSG
- Ulster University
- UniFida
- UNISON
- Unite
- United Kingdom Lubricants Association
- United Kingdom Security Vetting
- Universities Superannuation Scheme
- University College London
- University Hospitals Sussex NHS Foundation Trust
- University of Bradford
- University of Leeds DPO office
- University of Liverpool
- University of Strathclyde
- University of the Arts London (UAL)
- University of Winchester
- UNJUST C.I.C
- Unlock Democracy
- US-UK Business Council
- use MY data
- Veritau Group
- Victoria and Albert Museum
- Virgin Media O2
- Virtualgo2 Ltd
- Visa Europe
- Vodafone
- WaterAid
- WEA (Workers Educational Association)
- Wellcome Sanger Institute
- Welsh Government
- Welsh Revenue Authority
- West London Welcome
- West Midlands Fire Service
- West Yorkshire Police
- Which?
- William Reed Business Media Ltd
- Wise Parking Ltd
- Workday
- Xynics Data Solutions
- YouGov
- Your Homes Newcastle
- Your Housing Group
- Zorva Consulting Limited
- 3 Billion Pairs
- 360Giving
- 5Rights Foundation

Is this page useful? Yes No Report a problem with this page

OGL All content is available under the Open Government Licence v3.0, except where otherwise stated

© Crown copyright