# Chapter One: Reducing barriers to responsible innovation

17.12.2021

## 1.1 Introduction

No questions

## 1.2 Research Purposes

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

Somewhat agree

#### Q1.2.1a. Please explain your answer, and provide supporting evidence where possible:

Creating more specific research provisions within the legislation would make it easier for researchers to find a legal basis within the legislation, but only where an alternative is not available. For example, research teams within Local Authorities can rely on a variety of legal bases linked to the Public Task of the Local Authority. However, it would be useful to clarify the legality of re-use of data for research purposes that differ from the original purpose of collecting the data as this is often unclear.

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

Somewhat agree

#### Q1.2.2a. Please explain your answer and provide supporting evidence where possible.

Clarifying definitions and standards can help support researchers to understand the extent to which data can be shared or used. However, there is a concern that this may result in projects being ‘trimmed’ – reduced in scope or scale – to fit the statutory definition of ‘scientific research’. Similarly, this may encourage the inclusion of unnecessary additional partners (e.g. consultants or academics) to meet the statutory definition of ‘scientific research’, without initially considering their contribution to the work.

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

Somewhat agree

#### Q1.2.3a. Please explain your answer, providing supplementary or alternative definitions of 'scientific research' if applicable:

The definition of ‘scientific research’ in Recital 159 of the UKGDR is a good basis, but it is felt that this needs further clarity and additional definitions within it. Further definitional points to consider would include, but would not be limited to:

* How much ‘technological development’ would need to be shown?
* Would organisations need to show that research is fundamental, applied and privately funded at the same time; or can individual projects meet just one of these criteria?
* How much private funding would be needed to meet the criteria, and would this be expressed as a value or a percentage?
* What would be the definition of a ‘private funder’?

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

Strongly disagree

#### Q1.2.4a. Please explain your answer, and provide supporting evidence where possible, including by describing the nature and extent of the challenges.

The current law is clear enough. Research teams and organisations have clear guidelines from the ICO and other and implement processes to enable researchers to identify the lawful ground for personal data processing. Research should still be subject to relevant legislation and ethical practice. It is important to instil trust in research, and the lawful ground for collecting and using personal data helps to support that trust. Therefore, identifying a basis under which research is lawful enables the research to take place rather than produces a barrier. Legislation should assist in developing the outcomes of research and identifying what personal data is required for use and sharing as part of this.

There is a concern that loosening or broadening data protection legislation – especially around the lawful basis for research – could have a detrimental effect on conducting new and innovative research, if it led to individuals’ and businesses’ data are being used in ways that eroded public trust. For example, paragraph 30 of the consultation states “...the public being generally in favour of their personal data being used for scientific research that can deliver real benefits to society.” However, there are a range of studies also showing that consent is often withdrawn if individuals’ data is being used for profit. Examples of research on individuals’ attitudes to use of their data and consent include a [report from the Financial Services Consumer Panel from 2018](https://www.fs-cp.org.uk/sites/default/files/fscp_report_on_how_consumers_currently_consent_to_share_their_data.pdf) and [report from 2015 commissioned by the Direct Marketing Authority](https://www.fs-cp.org.uk/sites/default/files/fscp_report_on_how_consumers_currently_consent_to_share_their_data.pdf). There is also a [report from the ICO published in July 2021](https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/07/ico-publishes-annual-tracking-research/) which looked at what people think about data protection and information rights.

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

Somewhat disagree

#### Q1.2.5a. Please explain your answer and provide supporting evidence where possible.

To evidence a public task and how it is being supported, there needs to be a direct link to the work and outputs of central government, a local government organisation, or a public body. Evidence for this might include working alongside an appropriate public sector organisation. It is felt that allowing organisations outside of the public sector to unilaterally define their work as tasks in the public interest also provides scope to widen this definition without the input of central government, local government, or public bodies. This would appear to go against the spirit and general understanding of the definition of public task. It is felt, in particular, that the definition of public tasks is already clear enough to researchers, including universities and academics. Nevertheless, it may be useful to see changes to the legislation to include standalone university research.

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

Neither agree nor disagree

#### Q1.2.6a. Please explain your answer and provide supporting evidence where possible.

A separate, lawful ground for research (subject to suitable safeguards) could support researchers with suitable definitions and adequately assessed safeguards. By enshrining these in law, this would protect the personal data of the individuals, the academic or research bodies conducting the research, and any partners that might be involved. Furthermore, this would directly support trust in the public sharing information with researchers. Many public bodies are risk averse with regards to information. Changes to the legislation would help considerably in assuaging concerns around data being provided to external researchers. It may be useful to devise separate lawful ground in the same way that ‘legitimate interest’ is designed and exclude research which is undertaken for the purposes of public task. However, during the conversation within Greater Manchester about these proposals, participants from academia felt that the current law was clear enough and that their institutions had clear guidelines and processes to enable researchers and academics to meet the legal requirements and that this did not pose a barrier to research so the suggested reforms weren’t necessary.

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

It is felt that the production of mandatory Data Protection Impact Assessment should be built into the legal ground for research. This DPIA should describe the purpose; methodology; data to be used; level of anonymisation; and how and where the research will be made public (e.g., papers, journals, etc). It would also be useful to require an agreement to have any algorithms used within the research checked and verified externally. Where the use of AI and machine learning is used, an investigation into the limitations and possible false determinations that may arise should also be considered. Lastly, it would also be beneficial to require that those working in the research have training in current data processes and legislation, as well as information ethics.

### Q1.2.8. To what extent do you agree that it would benefit researchers to clarify that data subjects should be allowed to give their consent to broader areas of scientific research when it is not possible to fully identify the purpose of personal data processing at the time of data collection?

Neither agree nor disagree

#### Q1.2.8a. Please explain your answer and provide supporting evidence where possible.

Whilst this approach could benefit researchers by allowing further and wider uses of collected data, it is felt that this type of consent could not be described as ‘informed’. Therefore the individual would lose control of their personal data. This ‘uninformed consent’ could be detrimental to researchers as individuals may be less likely to provide consent for unknown research purposes, especially when compared to research where they know what is to be undertaken with their data. This would be particularly true for special category data such as health or criminal offence data.

If this model of consent for research were to be allowed, it is suggested that a requirement is built in to contact the individuals during the research if there is felt to be any use that may not have been apparent when consent was given. Ongoing monitoring of the consent would also be necessary to ensure that withdrawal of consent was straightforward for future uses of the data.

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

Strongly agree

#### Q1.2.9a. Please explain your answer and provide supporting evidence where possible.

Clarity is needed so that data subjects and researchers are clear what data they can use and when.

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

Somewhat disagree

#### Q1.2.10a. Please explain your answer and provide supporting evidence where possible.

It is felt that the current privacy notice approach is appropriate. If researchers use data outside the bounds of the original privacy notice for the collection of the information, then the individual should be informed whatever that extra use is and however difficult it would be to do. Data subjects have a right to know how their data is to be used.

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

One possible safeguard would be to require pseudonymisation or anonymisation (where possible) of the data collected, in order to provide some level of protection for individuals where they are unaware of what the further processing will be. Where we are dealing with large and complex data sets this anonymization may prove difficult, so this would require clear guidance on what would be required.

## 1.3 Further Processing

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

Somewhat agree

#### Q1.3.1a. Please explain your answer and provide supporting evidence where possible.

Whilst article 6(4) explains clearly what should be considered when determining whether further processing is compatible with the original purpose for which personal data have been collected, it does not provide any legislation on what the acceptable approach to these considerations is. As such it does not provide enough clarity, leading to confusion for the person applying it.

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

Somewhat agree

#### Q1.3.2a. Please explain your answer and provide supporting evidence where possible, including on:What risks and benefits you envisageWhat limitations or safeguards should be considered

It is agreed that the Government should seek to clarify when further processing may be lawful. In terms of safeguards, data subjects still need to know how their data is being used, even when being further processed. However, there is a potential risk that the public interest may not be reconciled between the data subject and the researcher. It is therefore important to apply a strong public interest test to ensure that the provision isn’t overused or misused. Furthermore, there is also still a need to define when public interest is applicable.

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

Strongly agree

#### Q1.3.3a. Please explain your answer and provide supporting evidence where possible, including on:

#### How you envisage clarifying when further processing can take place

#### How you envisage clarifying the distinction between further processing, and new processing

#### What risks and benefits you envisage

#### What limitations or safeguards should be considered?

To clarify when further processing can take place, criteria for the further processing would need to be specified, together with how that processing is linked to the original processing.

There is a risk that by sharing data for a specific purpose, data controllers would lose control of how that data was further processed. This would leave the data controller accountable for any third-party processing.  It would therefore be important to ensure that data controllers are able to control how the data they are responsible for is used, to safeguard the use of the data. This may involve limiting how far third parties can go with regards to the processing they intend to complete. Requiring a Data Protection Impact Assessment and a sharing agreement would also be a way to ensure this happens.

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

**Somewhat agree**

#### Q1.3.4a. Please explain your answer and provide supporting evidence where possible, including on:How you envisage clarifying when further processing can take placeHow you envisage clarifying the distinction between further processing, and new processingWhat risks and benefits you envisageWhat limitations or safeguards should be considered?

Consent must be informed, and able to be withdrawn and managed. As such, there is always a risk when using consent as a lawful basis, as the details of further processing will not necessarily be known when consent was given. The privacy notice or similar provided when consent is given should explain clearly where the research is intended to go and what safeguards are in place should the research scope widen because of discoveries made. There is a difficulty in balancing safeguarding the privacy of individuals and limiting the scope or scale of the research.  This is a difficult line to walk and legislation to clarify the situation would be welcomed.

## 1.4 Legitimate Interests

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

Somewhat agree

#### Q1.4.1a. Please explain your answer and provide supporting evidence where possible.

It is agreed that clarification would remove any ambiguity around the application of the test. However, there are concerns about creating an ‘exhaustive’ list, given the speed at which the landscape of data use within both public and private sectors is developing. This would likely need to be regularly reviewed and assessed to ensure that the list fully captures the range of legitimate interests.

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

Somewhat agree

#### Q1.4.2a. Please explain your answer, indicating whether and why you would remove any activities listed above or add further activities to this list.

There is general agreement in principle for the suggested list of activities. However, this would need to ensure that the risks are captured and managed as appropriate. For example, this might be captured in a Data Protection Impact Assessment, which would outline the benefits to the data subject as a matter of course.

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

As above (Q1.4.1) we would suggest that the list is regularly reviewed to ensure it remains appropriate for the expanding uses of data.

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

Somewhat agree

#### **Q1.4.4a. Please explain your answer and provide supporting evidence where possible**.

There is general agreement that personal information for children and vulnerable individuals should be subject to the balancing test. This is because children and vulnerable individuals experience an imbalance of power between themselves and the organisations who process their data. This can be evidenced by the ICO definition of vulnerable individuals within their DPIA guidance: “Individuals can be vulnerable where circumstances may restrict their ability to freely consent or object to the processing of their data, or to understand its implications”. As such it would be useful to ensure a legitimate interests balancing test is undertaken. This could be undertaken as part of a Data Protection Impact Assessment.

## 1.5 AI and Machine Learning

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

Somewhat agree

#### Q1.5.1a. Please explain your answer and provide supporting evidence where possible.

It is felt that the legal obligations are clear in terms of data protection, equalities, and procurement rules.

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

Somewhat agree

#### Q1.5.2a. Please explain your answer and provide supporting evidence where possible.

In terms of data protection, it is felt that the concept of fairness applies to AI in the much the same way as any other processing, but with the additional safeguards regarding automated decision-making. This is made clear in the legislation, and in the guidance produced by the ICO. It is felt that legislating specifically for artificial intelligence may prove difficult and risky, as technology will likely develop faster than the legislation can be updated. This can be demonstrated via the need in the early 2010s to update the existing data protection regime (DPA98 in the UK) as it had been written prior to several innovations in information technology.

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

It is agreed that, at a minimum, the ICO and the Alan Turing Institute should play a role in these assessments. The ICO have released a toolkit and documentation in partnership with the Alan Turing Institute specifically to support this. Furthermore the ICO currently have a call for information open on use of age verification software (which may include an element of AI) and this demonstrates the activity the ICO are undertaking to take these steps.

It is also important that relevant businesses – especially technology partners – should be involved and consulted. This is because these organisations are likely to understand the machine learning process and the potential for bias in AI systems.

It would also be useful to involve other public and private bodies with expertise in data ethics, such as the Centre for Data Ethics and Innovation.

The existence of these organisations evidences that the data protection regime currently in place is also the correct legislative regime to manage the use of personal data within AI.

### Q1.5.4. To what extent do you agree that the development of a substantive concept of outcome fairness in the data protection regime - that is independent of or supplementary to the operation of other legislation regulating areas within the ambit of fairness - poses risks?

Somewhat agree

#### Q1.5.4a. Please explain your answer, and provide supporting evidence where possible, including on the risks.

Within the public sector, where personal data is processed to produce fairness outcomes, the organisation is usually required to undergo an Equality Impact Assessment. This ensures that the organisation is meeting their equality duty under the Equality Act 2010, as the protected characteristics are broadly in line with that in the data protection regime. However, it is apparent that there are different characteristics listed under Article 12 of the Human Rights Act. It would therefore be a sensible move to bring all these lists together. This could be achieved by issuing more general guidance that is not simply limited to the processing of data by AI technology.

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

Somewhat agree

#### Q1.5.5a. Please explain your answer, and provide supporting evidence where possible, including which safeguards should be in place.

As the world moves towards using AI more to improve services, then the training and testing of AI needs to be as extensive and effective as it can be. The best way to do this is by providing more data for AI systems to learn from. This highlights several questions about risks:

Is the personal information secure whilst the system is learning, and afterwards?

Do people need to be informed that their information is being processed for this purpose, and if so, how?

Is there enough understanding about any biases being introduced into the learning process?

Will the users of the system understand the limitations of the output?

Who will understand the decision-making process?

How can the information rights of the individuals be exercised, if an AI system has learnt from that information?

It is felt that progress on using AI should not be blocked, providing adequate safeguards are in place to protect the security of the data, and data subjects are informed. It is noted that the ICO Sandbox approach is already in use for this kind of testing in a safe environment. This approach would be useful as it would provide a safe way to test and train the AI without risking compromising a live system. Testing using live data has the potential to affect the data within that system which could lead to detrimental outcomes for the data subject.

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

No

#### Q1.5.6a. Please explain your answer and provide supporting evidence where possible.

Local authorities, Housing authorities and the wider public sector in Greater Manchester are only using AI in a limited way at present, and so this issue has not been explored in depth. However, where it is in use, the lawful basis will most likely be the same as the existing legal basis for the local authority activity. For example, one local authority within GM uses AI to establish a level of funding support for individuals in receipt of Adult Social Care Services. The legal basis for this will be the public task of the organisation (as laid out in health and social care legislation), regardless of whether AI is used or not. Similarly two housing providers have started looking at how they can use AI to profile tenants safely by applying data minimisation measures. Again this would be undertaken under the existing legislation under which the housing authorities operate.

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

No

#### Q1.5.7a. Please explain your answer and provide supporting evidence where possible.

No issues have currently been experienced in navigating re-use limitations. However, AI development is in its early stages, and is being developed for very specific purposes. More widely, local authorities within Greater Manchester have also not yet experienced this challenge. However, there is significant experience in managing requests for data reuse, particularly for the evaluation of services or projects.

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

No

#### Q1.5.8a. Please explain your answer and provide supporting evidence where possible.

Local Authorities within Greater Manchester have not yet come across this challenge related to AI. However, as stated above in Q15.7a, local authorities are used to managing requests for data for the purposes of research. The use of AI is simply another method of processing that data.

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

Yes

#### Q1.5.9a. Please explain your answer and provide supporting evidence where possible.

The technology and approach have not been used very often within local authorities in Greater Manchester. Furthermore, the supporting documentation from the ICO is relatively new. As such, the IG aspect of the system can be cumbersome. However, it is expected that this will improve with time, and as the use of AI increases.

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

Somewhat agree

#### Q1.5.10a Please explain your answer, and provide supporting evidence where possible, including on:

#### The key benefits or risks you envisage

#### What you envisage the parameters of the processing activity should be.

It is agreed that clarifying the legal basis for bias monitoring, detection and correction would be useful. However, this may benefit more from expanding the focus, and not being limited to processing undertaken using AI. It is felt that it may be more impactful to consider a general legal basis for bias monitoring, detection, and correction. This would only be necessary where the bias is not linked to protected characteristics under the Equality Act 2010. Where these factors are concerned, there would be a reliance on the legal obligation ground of UK GDPR Article 6.

It is also important to consider more widely the use of bias as a way to expand the use of personal data and ensure that it is not used in an exploitative way. It is especially important to consider the context within which bias may occur.

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

Somewhat disagree

#### Q1.5.11a. Please explain your answer and provide supporting evidence where possible.

Bias monitoring needs to be completed competently and clearly. Without appropriate monitoring, AI systems can drift towards making opaque decisions, and potentially towards dangerous decisions. If it is not clear that personal data can be used for this purpose AI systems will soon become obsolete

However, it was felt that further clarity within the legislation is unnecessary. This currently falls under existing legislation (Schedule 1 paragraph 8), which provides a legal basis for ensuring equality of opportunity or treatment. Guidance on the application of this legal basis would cover AI as it covers any other type of processing.

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

Somewhat disagree

#### Q1.5.12a. Please explain your answer and provide supporting evidence where possible.

As in the response to question 1.5.11a, it is felt that this is unnecessary due to the existence of paragraph 8 of schedule 1 of the DPA18, which is a general provision to allow processing to ensure equality of opportunity or treatment. This would include ensuring AI does not introduce bias in the processing of personal data. Again, it is felt that AI is simply another method of processing personal data, and as such the general provisions cover AI already.

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

It is felt that the use of AI should be included in privacy notices relating to the processing of data. Further, the testing should be properly designed and evidenced, to identify attempts to reduce bias in learning. Testing should include periodic auditing of the outputs over time, in order to detect evolving bias.

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

Somewhat agree

#### Q1.5.14a. Please explain your answer, and provide supporting evidence where possible, including on:

#### The benefits and risks of clarifying the limits and scope of ‘solely automated processing’

#### The benefits and risks of clarifying the limits and scope of ‘similarly significant effects’

Article 22 should be read in conjunction with Recital 71 of UKGDPR. As with other articles that are somewhat ambiguous, it would be useful to incorporate the interpretation as included within the recitals more closely within the legislation. Any other clarification should be drafted in general terms so as not to limit the scope solely to AI, where possible.

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

Don’t know

#### Q1.5.15a. Please explain your answer and provide supporting evidence where possible.

N/A - don’t know of any alternatives

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

Neither agree nor disagree

#### Q1.5.16a. Please explain your answer, and provide supporting evidence where possible, on both elements of this question, providing suggestions for change where relevant.

It is felt that the article would seem to be future proof, but that the safeguarding statements are not particularly meaningful. Where the decision is authorised by a Union or member state (Article 22, 2(b)) there does not appear to be a declaration of the right to obtain human intervention, whereas this is explicitly stated for Article 22 2(a) and (c). It may depend on the circumstances of the processing as to whether human intervention would be desirable (by the data subjects). In addition, without a formal mechanism to provide the right to a review, it would still be likely that organisation would receive complaints or contact to services to ask why, for an example, an application had been unsuccessful.

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

Somewhat agree

#### Q1.5.17a. Please explain your answer, and provide supporting evidence where possible, including:

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

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

This would make the processing of personal data for automated decision making more consistent with other types of processing as defined in the existing legislation. However, removing the right for an individual to have the decision reviewed by a human would lead to erosion of trust for processing of this type, and could lead to significant negative effects for both individual and the organisation. For example a participant shared their experience of automated decision making when applying for a 0% balance transfer credit card to consolidate existing borrowing. Initially the automated process flagged that the individual already had a number of loans and credit cards. However, through human intervention the individual was able to explain to the bank that the purpose for the loan was not to extend borrowing further, but in fact was in order to reduce payments and clear the debt sooner. Without this human intervention the individual would potential have suffered financial hardship and would not have used this bank in the future due to the negative experience.

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

There are some concerns around the language used in the discussions of the definition and nature of personal data. These include the statement that “…personal data takes on a life of its own…” (chapter 105, page 42) and the suggestion of using Article 13 as a means to not disclose derived data. It is felt that this is not in keeping with an approach that puts “…the protection of people’s personal data…at the heart of our new regime…” (page 2).

If AI is used to profile or make decisions about individuals and they are not advised of the outcome, they would be unable to exercise their right to human intervention. Whilst it is understood that there is a complexity to providing this information, thought should be given to the way transparency can be achieved – for example, suggestions from engagement work conducted in Greater Manchester included the formation of an algorithm and AI register. The public cannot be expected to trust a system that makes decisions about them if they feel it is not transparent. It is felt that the approach should consider when and how individuals are given the output from the AI system, rather than whether the output should be given at all.

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

It is important to note that the examples provided about the demonstration of accountability are already within the UK GDPR. Recital 71 to Article 22, for example, states that data subjects should be able “to obtain an explanation of the decision reached”. It is felt that this needs to be more explicit and more widely available to the public through publication schemes and/or privacy notices. It would be beneficial, if organisations are unable to release this information about the systems, to explain why. A further suggestion would be to look to the FOI exemptions about release of system level data as an example. This will be key to gaining the trust of the public in the use of AI.

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

If AI is using personal data, it is felt that data protection legislation is the right framework. Appropriate due diligence is required, which would best be done through a DPIA. If there are limitations to how a DPIA can assess data driven harms when using AI, a suggestion would be that legislative guidance is issued on what should be included in a DPIA to ensure that support is provided for those assessing the harms. The DPIA is specifically used to identify, and risk assess “data-driven” harms. There is therefore no agreement with the proposition that this tool has limitations on the way it supports and documents assessment of these harms. However, we also recognise the value of Equality Impact Assessments in identifying bias affecting individuals with particular characteristics (as required under the Equality Act 2010). However, this would most likely be useful alongside rather than instead of a DPIA.

## 1.6 Data Minimisation and Anonymisation

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

Somewhat agree

#### Q1.6.1a. Please explain your answer and provide supporting evidence where possible.

It is now possible to use more advanced technology to compare data sets and look for patterns that may identify individuals. Individuals may also be identified by merging datasets to produce a data set as individual as a fingerprint without a name attached – this has been shown widely in the private sector’s use of data. Legislation should clarify that tests need to be done, but that how to test is dependent on the data being analysed. One example of this is the current work being undertaken by two housing authorities who are seeking to profile their tenants in a safe way by using data minimisation mechanisms, and it would be useful to have clarity around testing for anonymity in order to ensure this work is undertaken in the best way possible to protect the privacy of their tenants.

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

Recital 26 of the UK GDPR

#### Q1.6.2a. Please explain your answer and provide supporting evidence where possible.

It is felt that if clarity is to be provided, it should apply to all data processing, and not just related to automated processing as with Convention 108. By using Recital 26 as the basis, this would serve to bring the guidance into the legislation itself, thereby clarifying anonymisation and pseudonymisation with a legal footing.

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

Somewhat agree

#### Q1.6.3a. Please explain your answer and provide supporting evidence where possible.

It is felt that the legislation should place a due diligence requirement on the data controller to assess whether the anonymity of the data can be broken. This would include being broken internally and externally; by an individual or group who may legitimately have access to the anonymised data set; or by an individual that may work together to identify a data subject. For example, if working in partnership with a university that may have many research programs using many data sets, agreements should be in place to make sure that the data set is used according to a standard ethical practice, and that identification will not be attempted even as an academic exercise, without agreement with the data controller**.**

Undertaking this due diligence will be necessary to ensure full assessments are undertaken by controllers, making sure that the data remains anonymous, and protecting the rights of data subjects.

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

Article 25 of the UK GDPR requires organisations to take an approach to projects involving personal data that ensures “…data protection by design and by default”. Privacy-enhancing technology would go some way to meeting this, in some circumstances. It is recognised in the proposal that the ICO is shortly to publish guidance on its use. This shows that it is already the role of the regulator to promote this type of technology. There is currently no clear reason why this should need to change.

## 1.7 Innovative Data Sharing Solutions

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

No

#### Q1.7.1a. Please explain your answer, with reference to the barriers and risks associated with the activities of different types of data intermediaries, and where there might be a case to provide cross-cutting support). Consider referring to the styles of government intervention identified by Policy Lab - e.g. the Government’s role as collaborator, steward, customer, provider, funder, regulator and legislator - to frame your answer.

In the Government’s role as regulator, an accreditation scheme based on agreed standards of information security and records management would enable organisations to trust accredited intermediaries. It should only do this as regulator, and not as a provider, funder, or having been funded by data intermediaries.

### Q1.7.2. What lawful grounds other than consent might be applicable to data intermediary activities, as well as the conferring of data processing rights and responsibilities to those data intermediaries, where organisations share personal data without it being requested by the data subject?

It is noted that lawful grounds should be based on the purpose for processing data, rather than the method. Therefore, all the legal grounds in the legislation are available to this type of activity.

Conferring of data processing rights and responsibilities is already covered in Chapter IV, Section 1 of the UK GDPR. This is the responsibility of data controllers, determining if the processing is done by a third party acting as a data processor (responsibilities defined in Article 28 and 29 of UK GDPR); or in a joint data controller or separate controller relationship (Article 26 of UK GDPR). These definitions have been part of data protection legislation since the 1998 Act. Adding a third type of relationship that overlaps with these existing definitions is not only unnecessary but also introduces a level of complexity within the legislation that these reforms are aiming to overcome.

#### Q1.7.2a. Please explain your answer, and provide supporting evidence where possible, including on:

If Article 6(1)(f) is relevant, i) what types of data intermediary activities might constitute a legitimate interest and how is the balancing test met and ii) what types of intermediary activity would not constitute a legitimate interest

What role the Government should take in codifying this activity, including any additional conditions that might be placed on certain kinds of data intermediaries to bring them within scope of legitimate interest

Whether you consider a government approved accreditation scheme for intermediaries would be useful

It would be beneficial if the government could legislate for the creation of an accreditation scheme specifically for data intermediaries. This would include appropriate standards covering information security and records management, as examples. Furthermore, this would enable data controllers to trust intermediaries.

There is currently a service called ["rightly"](http://www.rightly.co.uk/) that offers a service to carry out individuals’ data subject rights. Currently, organisations who receive requests via this service have no way of knowing whether the service can be trusted to handle individuals’ requests. Most councils will refuse a request from a service like this, based on the advice of the Information Commissioner’s Office. This advice can be found in the  Guide to the General Data Protection Regulation in a section entitled “Do we have to respond to requests made via a third party online portal” (ICO Guidance found at  [ICO guidance on ‘Do we have to respond to requests made via a third party online portal’?](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/how-do-we-recognise-a-subject-access-request-sar/#portal_)). It includes ensuring that the organisation can be certain that the individual is who they are claimed to be, and that the service has appropriate authorisation. Without an accreditation scheme, the guidance recommends refusing a request from this service. Therefore, a list of trusted, accredited intermediaries would assist in being able to respond to these types of requests.

## 1.8 Further Questions

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

There are some concerns that the extended use of AI would introduce more bias against those with protected characteristics. This would be especially true if datasets were used from local public services to train AI systems. Some protected characteristics, such as disability and specific age ranges, are over-represented within local public sector datasets, as they are more likely to use public services. Comparatively, other characteristics are likely to be under-represented or not feature in the system - for example, religion or sexuality. However, as the use of AI is still at an early stage within local government, it is not yet known what the level of impact might be.

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

One potential reform would be to provide more detailed guidance to help inform a greater understanding of the current legislation, and how it could apply and be applied to different situations. This would have the biggest impact in reducing barriers.

Many of the barriers faced by the public sector, and researchers especially, can be reduced or removed completely if the legislation more widely understood and appropriately applied. The ICO undertake this role as regulator. It would be more beneficial to make existing guidance clearer, for example by incorporating the text of recitals within the operational text, rather than introducing new caveats and additions. The ICO role in providing advice and assurance should be strengthened to achieve this.

End of chapter Q. Do you have any general comments about this chapter not yet captured by your responses to the questions above?

As discussed above in several question responses, a central pillar of good data governance is that data subjects fully understand how their data will be used. Greater openness and transparency from organisations will help to build trust in the use of data, and in the use of new technologies. People can sometimes fear what they do not understand, and this can lead to a conclusion that data sharing as a whole is wrong. Research is a good example of this. If data subjects do not see the outcome of the use of their data, especially if part of a wider algorithm or AI training, they cannot understand how their data is being used.

Nevertheless, the current legislation does provide guidance and legal bases for conducting different types of data processing. It is felt that this does not currently pose a barrier to research, and reforms aimed at reducing or modifying the legislation are not currently necessary. Rather, greater guidance and assistance to clarify how legislation can be implemented across a multitude of project areas would support better application.