# **Chapter Four – Delivering better public services**

17.12.21

## 4.1 Introduction

No questions

## 4.2 Digital Economy Act 2017

### Q4.2.1. To what extent do you agree with the following statement: ‘Public service delivery powers under section 35 of the Digital Economy Act 2017 should be extended to help improve outcomes for businesses as well as for individuals and households’?

Somewhat Disagree

#### Q4.2.1a. Please explain your answer and provide supporting evidence where possible.

We consider that the current focus on improving outcomes for households and individuals is appropriate. Having reviewed the relevant part of the legislation and this section, it is not clear what if any additional power this gives businesses. We would have concerns if this would allow businesses to collect additional information for sharing, for example to open new avenues for internet providers (businesses which the act directly impacts) to collect more data from their customers. As such, it may be worth considering whether the term ‘business’ needs further definition. The consultation does not provide clear examples of where businesses have been impacted as a result of not having access to the power under S35 DEA where ordinarily it would have provided a solution.

Businesses working with public sector organisations in some contracted arrangements can rely on public task and thus where the public body is relying on public service delivery powers by extension the business can use these. However, this is only to the extent that delivery is line with the public bodies' identified outcomes.

## 4.3 Use of personal data in the COIVD-19 pandemic

### Q4.3.1. To what extent do you agree with the following statement: ‘Private companies, organisations and individuals who have been asked to process personal data on behalf of a public body should be permitted to rely on that body’s lawful ground for processing the data under Article 6(1)(e) of the UK GDPR’?

Somewhat Agree

#### Q4.3.1a. Please explain your answer and provide supporting evidence where possible.

This already happens. When commissioning Victim Support Services in GM to avoid the commissioned provider relying on consent, we liaised with the ICO who confirmed that the provider could rely on public task afforded to the Combined authority. This provided for a more streamlined service provision. However, there is some nervousness so something that is clear in the legislation would overcome this. This proposal is supported as it would strengthen Controller-Processor relationships within Local authorities and make it easier to justify and deliver services. It would make for a more streamlined and efficient means of processing personal data providing the purpose was distinctly clear with an unarguable Controller/Processor arrangement in place. This is on the understanding that it was clear any further use for their own ends or own purposes would not be permitted.

Freedom of Information (FOI) is not mentioned here. If a company is processing data on behalf of a public body, they should be subject to FOI.

### Q4.3.2. What, if any, additional safeguards should be considered if this proposal were pursued?

Assuming that all regular data processor agreements are in place that is processing on behalf and only for the data controller, erasure following processing, etc. We would like to see increased weight be placed on the legality and enforceability of the agreements if the above became common practice.

Clear, defined stringent instructions and rationale from the public body concerning the activity. Concerned there maybe a little mission creep though if too many private companies are given the opportunity of using public task versus other legal gateways.

More robust clauses in data processing agreements, with emphasis on the agreed/limited purposes for processing and data controllers may need to take a more active role in monitoring the contracts and the processing.

Public bodies should be required to very specifically define the task and timelines during which this is taking place. Loose definitions will allow private bodies a lot of flexibility.

Introducing more safeguards related to this is a great opportunity to consider requiring tasks and requests to be published openly. This will help people find these and become aware of who has access to their data which is important to help them exercise their rights.

### Q4.3.3. To what extent do you agree with the proposal to clarify that public and private bodies may lawfully process health data when necessary for reasons of substantial public interest in relation to public health or other emergencies?

Somewhat Agree

#### Q4.3.3.a. Please explain your answer and provide supporting evidence where possible.

Given the experience of the Covid-19 pandemic, and the potential for future emergencies, we support this proposal. It seems a pragmatic approach and only for emergency situations where it is a genuine belief that the public would have an expectation. However, clear differentiation needs to be made for the public and private sectors. In conjunction with a processor being able to use the controller’s justification, this lawful processing should only be available to public bodies.

There should be a requirement to very clearly identify and document the substantial public interest relied upon, why it is proportionate and necessary to carry out the processing to meet this and that it would not be contrary to the public’s expectations. During the Covid-19 pandemic there have been blockers to data sharing even in cases where there was no legal impediment. We need to have a significant conversation about the proper use of data (especially health data) in public health emergencies and then target legislative and other changes required

### Q4.3.4. What, if any, additional safeguards should be considered if this proposal were pursued?

We propose that the ICO should sign off any instances where this is deemed necessary and place a time limit on the power with continuous review where required that is like COPI.

Effective review mechanisms and conditional upon ensuring transparency with the public - either through privacy notices or other communications.

## 4.4 Building trust and transparency

### Q4.4.1. To what extent do you agree that introducing compulsory transparency reporting on the use of algorithms in decision-making for public authorities, government departments and government contractors using public data will improve public trust in government use of data?

Strongly Agree

#### Q4.4.1.a. Please explain your answer, and provide supporting evidence where possible

We strongly agree that transparency is important and given how ‘big data’ has already been used, we would fully support use of algorithms being transparent. We would also support that transparency being expanded to other sectors.

We do believe that there is a public concern on this issue and reporting would help in allaying fears that these are used routinely while ensuring that there is clarity on when they are used and the reasons that they are appropriate. It could bolster public confidence, trust and reassurance.

This has to communicated in plain language to help service users and communities understand this; conscious that not everyone has technical skills or knowledge in this space.

We would assert that there is a role beyond reporting on the use of algorithms post-implementation but build further on the consultative element of the Data Protection legislation and require public bodies to consult on their use.

Alongside ‘government contractors using public data’ it should include all those processing data on behalf of public bodies. Otherwise, there is a risk that data processing could be outsourced to those organisations without a requirement to be transparent in this way.

### Q4.4.2. Please share your views on the key contents of mandatory transparency reporting

Essential data protection considerations would provide a useful basis. For example, what is being collected, how data is being processed and what decision/s are being made.

### Q4.4.3. In what, if any, circumstances should exemptions apply to the compulsory transparency reporting requirement on the use of algorithms in decision-making for public authorities, government departments and government contractors using public data?

Exemptions should be applied only in very limited cases where data is highly sensitive, supports public protection or national security and transparency would seriously prejudice public interest

### Q4.4.4. To what extent do you think there are any situations involving the processing of sensitive data that are not adequately covered by the current list of activities in Schedule 1 to the Data Protection Act 2018?

Somewhat Agree

#### Q4.4.4a. Please explain your answer and provide supporting evidence where possible, including on:

#### What, if any, situations are not adequately covered by existing provisions?

#### What, if any, further safeguards or limitations may be needed for any new situations?

No comments.

### Q4.4.5. To what extent do you agree with the following statement: ‘It may be difficult to distinguish processing that is in the substantial public interest from processing in the public interest’?

Somewhat Agree

#### Q4.4.5a. Please explain your answer, and provide supporting evidence where possible

More clarity would certainly be beneficial as there is too little clarity in defining either term and more prescriptive direction, perhaps with examples, is needed.

### Q4.4.6. To what extent do you agree that it may be helpful to create a definition of the term 'substantial public interest'?

Somewhat Agree

#### Q4.4.6a. Please explain your answer, and provide supporting evidence where possible, including on:

#### What the risks and benefits of a definition would be

#### What such a definition might look like

#### What, if any, safeguards may be needed

A firm definition would make identifying what falls into this category more straightforward.

However, a risk is activities which rely on SPI but no longer fit the definition of it after further clarity may then be deemed non-compliant. Too strict a definition might impede lawful processing in situations where there is substantial public interest, but it doesn’t quite fit. Perhaps a broad, guiding definition would be helpful with some examples provided for in guidance.

### Q4.4.7. To what extent do you agree that there may be a need to add to, or amend, the list of specific situations in Schedule 1 to the Data Protection Act 2018 that are deemed to always be in the substantial public interest?

Neither agree nor disagree.

#### Q4.4.7a. Please explain your answer, and provide supporting evidence where possible, including on:

#### What such situations may be

#### What the risks and benefits of listing those situations would be

#### What, if any, safeguards may be needed

A consultation on the changes should be held on proposed changes to be made, not just a consultation on *if* changes should be made.

### Q4.4.8. To what extent do you agree with the following statement: There is an opportunity to streamline and clarify rules on police collection, use and retention of data for biometrics in order to improve transparency and public safety.

Somewhat Agree

#### Q4.4.8a. Please explain your answer, providing supporting evidence where possible.

We can see the importance of defining and being more prescriptive with how data is collected by the police and their methods to obtain it, process it and its retention. However, we would not like to see new measures in place that undermine the effectiveness of crime prevention and detection.

There is opportunity to clarify here. Having guidance and clarity on the use of biometrics in law enforcement is important on thew basis that it is used only for the purposes it is initially collected for.

The Government needs to also to consider emerging risks and opportunities related to biometrics. This section appears to be only mention of biometrics and there is no mention of implications of the growing use of genealogy tools such as ‘23AndMe’ and similar.

## 4.5 Public safety and national security

### Q4.5.1. To what extent do you agree with the proposal to standardise the terminology and definitions used across UK GDPR, Part 3 (Law Enforcement processing) and Part 4 (Intelligence Services processing) of the Data Protection Act 2018?

Neither Agree nor Disagree

#### Q4.5.1a. Please explain your answer, and provide supporting evidence where possible

Having standardised terms would make things clearer and will allow knowledge to be applied comfortably across Parts. It would be helpful to consolidate Parts 3 and 4 in particular as they both have chapters on principles and rights which are largely the same.

In reference to sharing between Parts 3 and 4, we are concerned that sharing between law enforcement and intelligence services should have significant checks and balances in place.

## 4.6 Further Questions

### Q4.6.1. In your view, which, if any, of the proposals in the chapter on 'Delivering better public services' would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

We can see a situation where immigration data (potential enforcement data; part 3) which will include race and possibly religious beliefs are shared with intelligence agencies (part 4) for national security and anti-terrorism purposes which would stem from broadening the use of SPI and allowing sharing between identified organisations.

### Q4.6.2. In addition to any of the reforms already proposed in the chapter on 'Delivering better public services' (or elsewhere in the consultation), what reforms to the data protection regime would you propose to help the delivery of better public services?

The chapter introduction describes a number of other significant challenges to data sharing related to the delivery of public services e.g. the lack of inter-operable systems, and differing capabilities. In this context, are the legal frameworks actually the key blocker at present.

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

The introductory section of the chapter talks about levelling up, net-zero and improving outcomes for education. However, these are not mentioned again throughout the rest of the chapter and so it is not clear how the proposals will affect these outcomes.

As part of the Greater Manchester engagement sessions commissioned by the GMCA, trust was repeatedly raised as being very important. It is discussed in the consultation, but the practical measures relate to a relatively narrow proposal around AI transparency.

More widely, attendees spoke of how they would like to see a visual of how data about them is flowing across the architecture of government and private/voluntary sector organisations processing on their behalf. Effort also needs to go into more straightforward and honest communication about use of data and GDPR which communities find hard to get to grips with.

A pro-growth strategy has to be balanced with communities and people, with consideration given to how communities can use data to help improve their local areas; to support the levelling up agenda.