Data. A new Direction On line Consultation Questions

1.REDUCING BARRIERS TO RESPONSIBLE INNOVATION

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?

○ Strongly agree

Somewhat agree X

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

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

We support these initiatives to drive further harmonization of laws applicable to the use of health data for research and innovation purposes and welcome further clarity around the definition of scientific research and extending the legal basis to enable industry access to data. We would recommend that policy makers address the following issues:

- Consistency with and ability to transfer health data with other appropriate international jurisdictions
- The legal basis for processing health data under the GDPR, and the interplay between the GDPR and the forthcoming UKCA regulations for medical devices and invitro diagnostics
- Guidelines on anonymisation and pseudonymization, and clarification when a data set can be considered sufficiently anonymised so it can be used and shared for research purposes (including commercial scientific research by medtech companies).
- The definition of "secondary use" should be clarified to enable the use of anonymised research data, for example medical images without patient information, to allow data processing for additional purposes that are not linked to the original study.
- exceptions for public interest and preventive medicine, in particular with regards to research conducted by medical technology companies;
- Clarity on any special category data provision which is an important distinction to make early in the defining of processing activities.
-

These recommendations are consistent with the recent publication by MedTech Europe 'Unlocking the full benefits of health data, dated June 16, 2021,

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

○ Strongly agree

Somewhat agree X

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

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

We appreciate that the Consultation supports clarifying a broad meaning for the term "research," as suggested by the UK GDPR recitals. Currently the legal basis is too narrow and only covers public health research. The advance of research in medical technology would benefit from clarity and legal certainty that the "research" provisions of the UK GDPR apply equally to private and public research projects. A statutory definition confirming this would support this.

The definition explicitly should include research by private parties as well as public universities or government institutions, especially where private parties perform research in accordance with related sector-specific methodological and ethical standards. It should also clarify any differences in approach for special category data and that the definition applies equally to research in a private setting. The current recitals to the UK GDPR do not appear to distinguish research conducted in an academic or commercial setting, and that references to clinical studies – which frequently are conducted by private sources – further implies that research in a commercial setting is within scope of the term.

It is highly important for the definition and scope of "research" under UK GDPR go beyond formal clinical studies to also include research on real-world evidence and secondary use of clinical trials data. These sources and uses are increasingly important to medical technology development, and their use both speeds and improves the quality of research purposes.

The definition and scope of "research" should also support the legal obligation of medical technology companies to engage in pre- and post-market clinical investigations and studies, which require the collection and processing of sensitive data. Additionally, MedTech companies have specific obligations regarding vigilance and safety reporting. This would require a broader interpretation of research than currently defined.

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

Yes X

No

Don't Know

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

The proposals encourage a broad interpretation of scientific research that extends to the areas of "privately funded research" and "technological development" (see Recital 159). The UK GDPR does not distinguish between research conducted in an academic versus commercial setting and references clinical studies when discussing research in the recitals to the law, implying that scientific research can be conducted in a commercial setting.

In circumstances where private research is utilising NHS data there would need to be clarity on who is the data controller in these situations, and who is responsible for the protection of the data. We further refer to our answer under Q.1.2.2a

.

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

○ Strongly agree

Somewhat agree X

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

1.2.4a. Please explain your answer, and provide supporting evidence where possible, including by describing the nature and extent of the challenges.

The overarching requirement to identify a legal basis for processing is a safeguard against misuse of data and should remain in place. Further clarity of legal certainty around the appropriate legal basis (art. 6 UK GDPR) and condition for processing (art. 9 UK GDPR) would address issues experienced by MedTech companies with regards to access to data for research, both relating to clinical research (research on humans) and non-clinical research (on data, e.g. computer modelling and simulation) and re-use of health data.

Work to align sector-specific regulation (UKCA mark for medical devices and invitro diagnostics) would be beneficial. It is unclear to what extent these regulations can serve as a stand-alone condition for processing under art. 9, 2, i) and j) of GDPR, for the processing of health data by medical technology manufacturers. There is a need for consistency and further clarification of the interplay of the UK GDPR and the UKCA regulations, and how medical technology companies can use the regulations as a legal basis to process personal data under the GDPR.

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

○ Strongly agree

Somewhat agree X

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

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

Creating an additional lawful basis for the use of (health) data for research purposes may be beneficial, for example if a broad statutory definition of research and/or a list of agreed legitimate purposes would not be sufficient in isolation to remove the challenges that researchers in the MedTech industry face when identifying an appropriate condition for processing under art. 9 UK GDPR. Suitable safeguards would need to be put in place and issues regarding the use of anonymised/pseudonymised data would need to be clarified and subsequent retention periods and limitations of processing need to be defined.

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

Safeguards to consider are a data governance program that manages and ensures accountability for health data processed for research purposes. Measures that might be incorporated here are a data governance board that oversees how and when health data are used based on the legal ground for research. This must be accompanied and strengthened by organisational measures and efforts to build a culture of privacy within the organization. Measures that could support this are internal policies and procedures

Technical measures can include encryption and other cryptographic tools, as well as role-based access controls and other measures. Both the technical and organisational can be assessed and implemented in comparison to the risks associated with the data processing operations.

Per Article 89(1) UK GDPR and the corresponding recitals, data minimization techniques, such as anonymisation and/or pseudonymisation are safeguards relevant to consider as well, taking into account that:

- MedTech companies will rarely use other than key-coded or pseudonymised datasets for scientific research purposes;
- Full anonymisation may not in all instances be an option, as datasets may lose their scientific value when very intrusive anonymization techniques are applied.
- It should be noted that part of the problem contributing to the situation of legal unclarity, is the lack of international consensus on appropriate de-identification standards for health data for research purposes.

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

Strongly agree

○ Somewhat agree X

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

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

We would welcome clarity on the scope of 'broader areas of scientific research' and if it includes medical research using special category data and if so any particular additional requirements that may be needed to utilise this type of data on a broad consent basis. It would be helpful if examples or guidance could be developed on this topic, such as on what level broad consent can be permissible.

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

Strongly agree

○ Somewhat agree

○ Neither agree nor disagree X

○Somewhat disagree

○ Strongly disagree

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

While we agree with the principles outlined we need further clarity regarding

- The role of controllers and processors and ability of the latter to invoke compatibility if the further processing of health data is for scientific research purposes.
- Where further use does not fit the concept of research purposes, how to assess and how to document compatibility assessments
- Guidance on how to further process health data where compatibility would not apply; this could be either after anonymisation or processed as necessary for scientific research purposes
- What guidance will be provided to researchers to judge subjectively?
- Will researchers be able to share that data with other researchers under that legal basis

A framework needs to exist that defines how far from the original data processing purpose any subsequent research can diverge.

Where health data is originally collected on the basis of consent, this should not exclude the possibility to rely on compatibility when the further use is for research purposes. The UK GDPR did not exclude personal data collected on the basis of consent from the application of art. 5, 1, b). Rather than deviating from the text of the UK GDPR in the upcoming initiatives, it would be helpful if the upcoming initiatives confirm the assumption of compatibility, provide clarity on the concept of research and appropriate safeguards for the assumption to apply.

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

A data governance program that manages and ensures accountability for health (special category) data processed for scientific research purposes under the exemption regime, can be a useful component, this should also take account of additional sensitivities over paediatric data. Measures that might be incorporated here are a data governance board that oversees how and when health data are used under the exemption provisions. This must be accompanied and strengthened by organisational measures and efforts to build a culture of privacy within the organization. Measures that could support this are internal policies and procedures supported by use of recognised standards.

Technical measures can include encryption and other cryptographic tools, as well as role-based access controls and other measures. Both the technical and organisational can be assessed and implemented in comparison to the risks associated with the data processing organizations, as required for example by Article 35 UK GDPR.

Per Article 89(1) UK GDPR and the corresponding recitals, data minimization techniques, such as anonymization and/or pseudonymization are safeguards relevant to consider as well, taking into account that:

- Medtech companies will rarely use other than key-coded or pseudonymised datasets for scientific research purposes;
- Full anonymization may not in all instances be an option, as datasets may lose their scientific value when very intrusive anonymization techniques are applied.

It should be noted that part of the problem contributing to the situation of legal unclarity, is the lack of international consensus on appropriate de-identification standards for health data for research purposes. Further clarification of when a data set can be considered sufficiently anonymised so it can be used and shared for research purposes (including commercial scientific research) would be valuable.

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?

Strongly agree X

○ Somewhat agree

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

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

Establishing a limited, exhaustive list of legitimate interests for which no balancing test would be required would substantially support innovation and the development and use of medical technology in the UK. It is critical that mechanisms exist to keep this list contemporary so as not to limit future. We also believe that there may be an opportunity to provide sector-specific legitimate interests, in addition to the general menu available to all. The current legislation contains extensive documentation obligations, such as the obligation to have an appropriate policy document in order to meet a UK Schedule 1 condition for processing in the DPA 2018 – an obligation which typically does not exist in other jurisdictions subject to the EU GDPR. The Government's proposal to create such a list would reduce the burden of those documentation obligations, while increasing legal certainty about when it is possible to rely on the lawful ground of legitimate interests under Article 6(1)(f) of the UK GDPR.

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

○ Strongly agree

Somewhat agree X

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

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

We support the proposal that any list of data processing activities (where the balancing test would not be required) need to be sufficiently generic to withstand the test of time. In that respect, the suggested list of purposes is a useful starting point. However, we suggest it would be helpful to give a more comprehensive list. For example, the purpose "monitoring, detecting or correcting bias in relation to developing AI systems" in paragraph 61(c) should be broadened to explicitly cover the training and testing of such systems. Similarly, the purpose "using audience measurement cookies or similar technologies to improve web pages that are frequently visited by service users" in paragraph 61(d) should be broadened to cover the use of such cookies and technologies on both websites and apps for "audience measurement". The term "audience measurement" is a widely used term that can cover many operations such as troubleshooting/detection of browsing issues, optimisation of technical performance or ergonomics, estimation of the server power required, and analysis of visited content, which could be specified in ad hoc guidance.

Because the health sector is a major field for use of data for legitimate, beneficial purposes, it would be useful to add a specific Legitimate Purpose for healthcare. Such a purpose could state,

"Healthcare purposes, including care delivery, healthcare management and operational improvement, monitoring healthcare safety and effectiveness, meeting healthcare regulatory requirements, and healthcare and health technology research and innovation".

For reasons of completeness, we add that it is not sufficient to only address the possibility of legitimate purpose as lawful basis under Article 6 of the UK GDPR, but also it will have to be clarified what appropriate condition for processing in Article 9 of the UK GDPR MedTech companies can use to support the processing of health data for the listed legitimate purposes.

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

We do not expect that additional safeguards would be required. This is because broader protection principles and safeguards would continue to apply, such as the obligation to carry out a DPIA, where appropriate.

By analogy with the DPIA requirement under the EU GDPR, some EU supervisory authorities have published whitelists of data processing activities that do not require a DPIA. When doing so, they have typically not required additional safeguards.

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

○ Strongly agree

○ Somewhat agree X

Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

The personal data of minors needs to remain protected. While the UK GDPR recognises that particular care should be taken when processing children's data, broader protection principles and safeguards would continue to apply, where appropriate. Under current regulations, organisations may have the freedom to independently define what ages are regarded as minors. Any clarification and concreting ruling on this would be welcome.

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?

○ Strongly agree

Somewhat agree X

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

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

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

○ Strongly agree

Somewhat agree X

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

Please explain your answer, and provide supporting evidence where possible

The main issue here is not UK GDPR itself, where fairness is well understood, but in the context of a wider definition of 'outcome fairness' in, where there is no always alignment with other legislation such as consumer protection, employment, equality, human rights law and sectorial regulations

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.

In principle we welcome initiatives to clarify the definition of 'outcome fairness'. For the medical technology sector we strongly recommend this should be done with in the framework of the medical device and invitro diagnostics regulations.

In the medical technology sector outcomes fairness needs to be evaluated in light of the existing and planned frameworks and enforcement mechanisms for the safety and performance of medical technologies, including those that comprise, or incorporate AI. These include, for instance, dedicated rules on risk management, quality management, technical documentation, and conformity assessment. The existing framework and regulators (MHRA) are best placed to determine how the concept of "outcome fairness" applies to the sector, and the necessary regulatory requirements that need to be set out in that regard.

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

Strongly agree X

○ Somewhat agree

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

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

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

Yes X

No

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

It is arguable that use of data for initial development and training of an AI algorithm could be considered "research," however it is unclear if the research provisions of UK GDPR extend to use of data for testing, validation, and continuous improvement of algorithms. As stated earlier we would recommend a broad definition of research to encompass such use cases.

Further, relying on individualized consent, exceptions for anonymised data, or exceptions for "research" may not fully authorize these AI-related data uses. For that reason, we support the Government's proposal in Paragraph 54 of the Consultation to allow certain secondary uses for an affirmatively specified legitimate purpose.

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

Strongly agree X

○ Somewhat agree

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

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

We support the proposals and also recommend supplementing such a list with clear and manageable data use requirements.

We share the Government's view that making explicit consent a prerequisite for data access and use for bias detection and mitigation purposes may in itself risk introducing bias into the data used in an AI system, furthering the risk of introducing unwarranted bias in AI algorithms used in medical technology.

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

Strongly agree X

○ Somewhat agree

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

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

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

○ Strongly agree

Somewhat agree X

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

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

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

Q1.5.16. To what extent do you agree with the following statement: 'In the expectation of more widespread adoption of automated decision-making, Article 22 is (i) sufficiently future-proofed, so as to be practical and proportionate, whilst (ii) retaining meaningful safeguards'?
○ Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
Strongly disagree X
Please explain your answer, and provide supporting evidence where possible, on both elements of this question, providing suggestions for change where relevant.

ABHI agrees with the lack of clarity on practical implications of Article 22 of UK GDPR, in particular in relation to the meaning and scope of "solely" automated decision-making as opposed to general automated systems.

We believe the risks presented by automated decision-making systems are already addressed in medical device and invitro diagnostic sectorial regulations which stipulate that medical device manufacturers (including those AI-enabled) demonstrate their device's safety and performance based on its intended use. This entails ex-ante as well as ex-post controls on the safety and performance of medical devices (throughout the entire device lifecycle). The design of the device must factor in its normal use conditions to ensure it performs as per expectations under clinical conditions and does not compromise the safety of the patient. It also entails that decisions pre-defined by AI-enabled products are "explained" as to make them trusted and useful to the user (physician or patient) and to ensure the device's safe and effective use.

Therefore, we:

- recommend that, rather than taking the "blanket" approach of Article 22 of UK GDPR, sectorial regulations establish clear transparency requirements applicable to AI applications to ensure that actionable information is provided to the user as to guarantee safe and effective use of the product;

- concur with the Taskforce on Innovation, Growth and Regulatory Reform's recommendation that Article 22 of UK GDPR be removed, and that the use of solely automated AI systems be permitted on the basis of legitimate interests or public interests, subject to appropriate sectorial regulations.

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

○ Strongly agree

○ Somewhat agree X

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

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

- The benefits and risks of the Taskforce's proposal to remove Article 22 and permit solely automated decision making where (i) it meets a lawful ground in Article 6(1) (and, Articles 9 and 10, as supplemented by Schedule 1 to the Data Protection Act 2018) in relation to sensitive personal data, where relevant) and subject to compliance with the rest of the data protection legislation.
- Any additional safeguards that should be in place for solely automated processing of personal data, given that removal of Article 22 would remove the safeguards currently listed in Article 22 (3) and (4)

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

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?

Strongly agree X

○ Somewhat agree

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

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

We welcome the proposal for legislation to make data anonymous relative to the means available to the data controller to re-identify it and would favour option 1 (placing the text from Recital 26 of the UK GDPR on to the face of the legislation). Clarification on the definition of "anonymisation", "anonymous data" and "de-identified data" would be useful additional guidance. A distinction should be made between "anonymous data" (i.e., data that is not personal data) and 'anonymised data' (i.e., data that is no longer personal data because it has undergone processing to render it anonymous). We also recommend further clarification when a data set can be considered sufficiently anonymised so it can be used and shared for research purposes (including commercial scientific research by MedTech companies). The definition of "secondary use" should be clarified to enable the use of anonymised research data, to allow processing for additional purposes that are not linked to the original study.

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.

Anonymisation is not the only privacy-friendly way to harness the potential of data, and the Government should promote and support privacy-enhancing technologies (PETs), such as federated learning and synthetic data generation, to explore new opportunities and boost innovation, while mitigating data protection risks. In that respect, it would be beneficial if the Government encourages the ICO to provide clear guidance to help organisations build confidence in the use of emerging PETs. It would be all the more important in the medical technology industry, where - for digital health to reach its full potential, we need to unlock the benefits of health data. Moreover, it should be clear when pseudonymisation or PETs are mandated, versus when they simply offer additional protection for data subjects. For example, PETs may be applied as part of a privacy-by-design approach, but it remains unclear how an organization might validate that they are sufficient. Technical standardisation could also help organisations to develop these approaches themselves.

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

○ _Yes X

○ _No

○ _Don't know

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

We support the creation of data intermediaries (such as Trusted Research Environments) in particular for data hosted by public bodies, such as the NHS. We are in favour of fair access terms that are not discriminatory between requests from public sector versus private sector. Mechanisms for enabling access of health data hosted outside the NHS for the purpose of scientific research needs to be articulated including how to add those datasets to those hosted in NHS research environments.

2. REDUCING BURDENS ON BUSINESSES AND DELIVER BETTER OUTCOMES FOR PEOPLE

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

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

Strongly agree X

○ Somewhat agree

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

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

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

- Would the adjustment provide a clear structure on when to report a breach?
- Would the adjustment reduce burdens on organisations?

What impact would adjusting the threshold for breach reporting under Article 33 have on the rights and freedoms of data subjects?

Strongly agree X

○ Somewhat agree

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

This approach would help build trust and transparency and increase the number of companies coming forward and notifying the ICO of infringements without fear of enforcement action.

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

○ _Strongly agree
○ _Somewhat agree
○ _Neither agree nor disagree
○ _Somewhat disagree X
○ _Strongly disagree

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

We recommend that it is further looked into to what extent this may put at risk the current adequacy agreement with the EU. This adequacy agreement is an important mechanism for data sharing for our sector.

4. DELIVERING BETTER PUBLIC SERVICES

4.3. Personal Data Use in the COVID-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'?

Please explain your answer, providing supporting evidence where possible.

Strongly agree

○ Somewhat agree X

○ Neither agree nor disagree

○ Somewhat disagree

○ Strongly disagree

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

In many cases, assuming that where the outsourcing of public tasks to the private sector involved the processing of personal data, then the private sector entity in that case would be acting as a data processor. Where the private company is a data controller, there is a logic in allowing that private company to rely on the public sector's lawful ground under Article 6(1)(e). This would raise important considerations for the private sector entity; for example; how would the private sector entity receive assurance that the public body had appropriately assessed the lawful ground? If the public body was found by ICO to have erred in its assessment, how would the private sector entity be impacted? These issues could be addressed through contracts which could take a standardised form.

We agree with ICO comments that the private sector entity should not be entitled to rely on this lawful ground to reuse the data for other purposes.

We have reservations about extending FoI requirements to private sector entities in these circumstances. The private sector is ultimately processing data on behalf of the public entity, who remains responsible for identifying and applying the appropriate lawful ground for processing. If private entities become subject to the same transparency requirements as public entities, via FoI, when they are carrying out public tasks on the public sector's behalf, this is likely to add greater compliance burden.

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?

Please explain your answer, providing supporting evidence where possible.

Strongly agree

○ Somewhat agree

○ Neither agree nor disagree X

○ Somewhat disagree

○ Strongly disagree

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

Clarification of what processing in the substantial public interest means in these circumstances, for example, what is the nature of public health or emergency which is envisaged?

Safeguards to give public confidence that their sensitive healthcare data means.

Scope for mis-use, and deliberate misinterpretation of what may be a reason of substantial public interest in the context of an emergency. Scope for uncertainty by data controllers.

Should be for a specific and time-limited purpose. Confidentiality should be retained.