Consultation response: Data Protection

phg foundation
making science work for health

Submitted to

Department for Digital, Culture, Media & Sport

Submitted by

Dr Colin Mitchell
colin.mitchell@phgfoundation.org

November 2021

The PHG Foundation welcomes the opportunity to comment on this consultation on reforms to the UK data protection regime. We are a health policy think tank with a focus on genomics and innovative health technologies, and over the last five years we have conducted significant research on the interaction between data protection law and genomic data in healthcare and research.

In 2017 we published the report Identification and genomic data and in 2020 we published a comprehensive report from our year long ICO-funded research on the impact of the GDPR on genomic data processing in healthcare and scientific research. In this research we conducted legal analysis, stakeholder interviews and convened an expert meeting of specialists in genomic data, health, research and data protection to identify the key impacts of the GDPR on genomic data processing. Alongside this we have also carried out significant research on the development of AI tools in healthcare, including the extent to which the GDPR requires machine learning in the context of healthcare and research to be transparent, interpretable, or explainable. These resources are freely available on our website.

Drawing on this and subsequent research, we have responded to the consultation questions and uploaded our answers to the online platform. However, we would also like to make some supplementary general comments that cut across multiple aspects of the proposals and different sections of the consultation document.

The importance of a continued 'adequacy decision' for the UK

An overarching concern is that the proposals risk diverging sufficiently from the European Union's standards that the UK will be adjudged to offer a lower (and inadequate) level of protection for personal data. This would jeopardise free flows of data between the UK and the EU, which are crucial to scientific and genomic research in particular.

The UK does not need to maintain an exact copy of the EU GDPR but we are concerned that some of the proposals could be viewed as sufficiently divergent to impact on adequacy. For example, the proposal to adopt a statutory test for anonymisation could lead to a view that the UK regime has a fundamentally different scope of 'personal data' to the EU. If this is narrower, it will de facto be viewed

as offering lower protection. In our research we identified a range of challenges that EU/EEA collaborators faced agreeing and authorising international transfers of data outside the EEA. These included different views about whether data are 'personal data' or not, causing significant harm to international research collaborations in certain cases. At present the UK is not suffering from the same level of friction but this is at stake if reforms are brought forward to adjust the framework without due regard for the impact on adequacy.

Evolution not revolution

Allied to this challenge, we advocate for a gradual process of adjustment to our data protection laws, based on broad and deep consultation with relevant sectors, to ensure that the proposals will not unnecessarily impact international flows of data and will not lead to unwarranted lowering of the level of protection afforded to fundamental data protection and privacy rights. It is difficult to do justice to the novel proposals within this consultation given its breadth and length. We hope that this consultation is a starting point for continuing engagement about what is being proposed, and not the final opportunity for comment, especially since our lack of comment does not reflect a lack of familiarity with the context or relevant law but because we do not have resources to give each aspect the consideration that it is due.

Improving data protection for research

We strongly welcome the focus of this consultation on the impact of data protection on scientific research processing. We think many of the barriers identified and a number of the suggestions in this area are sensible. However, we question the strength of some of the claims made about the role of law as a barrier in these proposals. In our research, we identified that uncertainty and complexity were the key and overarching challenges for researchers. However, we recognised that both of these are inevitable in the application of a comprehensive and sector-agnostic new law.

Our work highlights that the challenge is not the wording of the law (although there are undoubtedly aspects that could be better drafted) but rather the inevitable scope for argument about its proper application in a specific context, such as genomic research. To change the law would be unlikely to significantly alter the scope for that argument. We recommend that as much resource and effort as possible is put into developing specific guidance, in consultation with relevant industries and sectors to address these challenges, rather than changes to the legislation.

The importance of the ICOs role and specific guidance

In our research we found considerable approval for the ICO's track record in producing user friendly and sensible guidance. What is required is resources for this to be expanded and updated to address

new challenges. An obvious area for continuing and updated ICO guidance is de-identification and technical approaches to privacy preservation. If the ICO can keep pace with the state of the art this will give greater confidence to data controllers and subjects about the measures put in place to reduce (but almost never eliminate) threats to privacy. We strongly refute the concept of a 'surfeit of guidance' in this regard. The ICO's position means that its guidance is more authoritative than guidance, principles or technical documents that may be produced by non-regulatory bodies.

Innovation, trustworthiness and data governance

As a policy think-tank championing the role of innovation in improving population health we welcome the Government's ambition to support innovation, particularly in our field of health. However, we believe that the UK's record is and should continue to be as a world leader in safe, effective and ethical innovation. This requires proportionate regulation that ensures controllers, such as AI developers, act in ways that demonstrate their trustworthiness and maintain the support and confidence of the public. As we address in our latest research on changes to the regulation of confidential patient information during COVID-19, public trust and confidence is paramount. A loss of confidence can critically harm health research in particular, or even faith in the healthcare system.

Data protection law is only part of this picture. Alongside other areas of law and governance, including the common law of confidentiality, consumer protection and professional negligence, the goal of any reforms should be to safeguard fundamental rights and freedoms while supporting ethical innovation. This extends to aspects that are largely outside the realm of data protection. Notably the governance of non-personal data, addressing the challenges of opaque or adaptive high-risk AI, and addressing group, as opposed to individual, impacts. If this is successful, law and regulation will play an important role in supporting, not hindering innovation.

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 disagree

The PHG Foundation has conducted comprehensive research into the impact of the GDPR on genomic research. While we identified significant uncertainty on the part of researchers we are cautious that consolidating provisions would be beneficial. This is because it may in fact lead to greater uncertainty for researchers collaborating with European partners if the relevant provisions lose alignment with their position in the EU GDPR which could potentially have a stultifying impact on the sector hindering activity and investment.

Moreover, we concluded that the primary challenge was not the law itself, which is inherently complex and uncertain as it governs all 'personal data' processing across all sectors, rather it is the uncertainty in how it should apply in specific contexts, such as scientific and genomic research. We do not believe that this uncertainty would be best addressed through legislative change because the wording of the law and its application to new developments in this highly dynamic field will always be subject to debate and interpretation. Instead, we conclude that the solution is in the development of authoritative guidance on the correct application of the law in specific contexts. The ICO has an excellent record in producing user friendly and robust guidance. We suggest that the ICO should be resourced to develop appropriate guidance in consultation with relevant sectors, such as the genomics sector, in a way that ensures appropriate standards for those sectors and maintains a high level of protection for personal data.

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

Somewhat disagree

The PHG Foundation has conducted comprehensive research into the impact of the GDPR on genomic research. We concluded that the primary challenge was not the law itself, which is inherently complex and uncertain as it governs all 'personal data' processing across all sectors, rather it is the uncertainty in how it should apply in specific contexts, such as scientific and genomic research. We do not believe that this uncertainty would be best addressed through legislative change because the wording of the law and its application to new developments in this highly dynamic field will always be subject to debate and interpretation. Instead, we conclude that the solution is in the development of authoritative guidance on the correct application of the law in specific contexts. The ICO has an excellent record in producing user friendly and robust guidance. We suggest that the ICO should be resourced to develop appropriate guidance in consultation with relevant sectors, such as the genomics sector, in a way that ensures appropriate standards for those sectors and maintains a high level of protection for personal data.

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?

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

No.

As above we do not feel it is not appropriate to set out a statutory definition but better to develop guidance which can expand on this. We also note that the recital currently refers to a 'broad' definition of scientific research and it is perhaps more appropriate to maintain a broad scope but to ensure the law and guidance sets appropriate safeguards and standards for all activity within that scope.

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

Somewhat disagree

In our research we found that there was some uncertainty and difficulty identifying a lawful basis for processing for research projects which involved international and cross border collaboration in particular. However, there was less evidence of this difficulty in the UK where public sector researchers could rely on Art 6(1)(e) and those in private organisations could rely on Art 6(1)(f). The central challenge with legal bases that we identified related to changes in guidance relating to researchers' reliance on consent as a legal basis for data processing research. It has taken some time for researchers to adapt to this change, and more work is needed to communicate the rationale for this change. However, it does not appear that there is an absence of an appropriate legal basis for research, instead there is continued need for advice and guidance on the complexity of the law for researchers.

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 agree

We agree that further clarifying in guidance the circumstances in which university researchers can rely on Art 6(1)(e) could be helpful. However, there is already good guidance from the ICO and NHS Health Research Authority on legal bases and we have not identified this challenge as part of our research on the impact of the GDPR. There should be consideration of whether further guidance is necessary or whether it could lead to an even more complicated landscape for university researchers and potentially the erosion of public trust if this ground was used for research that is not perceived as being in the public interest.

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?

Somewhat disagree

We found no evidence in our study that there was a gap in the existing legal bases for research. We identified challenges with consent but that there were suitable alternative legal bases in Arts 6(1)(e) and 6(1)(f) in particular for research. Again, the challenge lies in understanding the requirements and limitations of different legal bases (and in their implications in terms of corresponding data subject rights and duties) and this would be better addressed through targeted guidance for public and private sector researchers.

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

If a separate lawful basis is provided for research, it will be important to ensure that there are safeguards which provide for appropriate ethical review of research in medical and biomedical research using personal data. It may also be appropriate to limit the scope of such a lawful basis to research in the public interest to guard against commercial and private interests driving forward research in a way that would undermine public trust and confidence.

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?

Somewhat agree

In our research we identified uncertainty on the part of researchers about the breadth of permissible consent under the UK GDPR for research purposes. This is also subject to ongoing academic debate (e.g. Hallinan, D. Broad consent under the GDPR: an optimistic perspective on a bright future. Life Sci Soc Policy 16, 1 (2020). We agree that it may be helpful to clarify that broad consent may be appropriate in certain areas of scientific research in targeted guidance which assists researchers to recognise when this may appropriately apply. However, we are cautious about the divergence this may create with EU data protection standards and the potential for this to impact the current EU-UK adequacy agreement. We are also concerned that this may not assist international collaborations where different understandings of consent could prove problematic. Although it may be unhelpfully confusing to have to explain that consent is a legal basis for disclosure of confidential patient information but is not relied upon under the UK GDPR, there are better legal bases available for most forms of research in the UK (unlike some EU countries). In particular, given the revocability of consent under the UK GDPR and the difficulty this creates in justifying the fairness of relying on an alternative legal basis for researchers, it is likely (and recommended by the NHS Health Research Authority) that other legal bases will be preferable for scientific research.

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?

Somewhat disagree

This question elides two separate principles of data protection and different requirements under the GDPR/UK GDPR. The principle of purpose limitation is modified in the case of research (in accordance with Art 89) so that further processing will be deemed compatible. It would be beneficial for this to be communicated to researchers.

However, it is not necessarily the case that research requires no new or newly justified legal basis for further processing. There is no modification of the principle of lawfulness in the text of the UK GDPR and the recital is ambiguous in its meaning (and non binding in law). To assert that further processing for research purposes is automatically lawful under Article 6 could be wrong in law (if the UK GDPR is not modified to provide for this). It would also remove the requirements to consider the fairness of choosing an alternative legal basis if the original legal basis was consent or of conducting balancing tests to justify the necessity of processing under Art 6(1)(e) or (f) for example, and a legitimate interest assessment under Art 6(1)(f). There should be caution in removing these safeguards without due consideration.

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 agree

We agree that the same exemption for further processing for research purposes should be provided under Art 13 as under Art 14. Our research identified this inconsistency. However, this may not be so significant as Art 12 does not necessarily require direct personal 'recontact' but instead requires that information is 'provided' in an easily accessible form. We agree with the ICO guidance that this requirement can be met by putting information on a website, making individuals aware of it and providing an easy way to access it. This means that the effort required may not be as great as direct and individual contact for each individual may imply.

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

The safeguards required should echo those in Article 14, namely: a

limitation to circumstances where the obligation to inform would be likely to render impossible or seriously impair the achievement of the objectives of the processing and a requirement to take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

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?

We somewhat agree that it is not easy to determine compatibility but again, it may be better to address this through guidance to assist controllers rather than changing legislation. Purposes limitation is a component not only of the GDPR but also of the Council of Europe's Convention 108+.

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?

Neither agree nor disagree

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

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

Again, our research has not identified any evidence from the scientific and genomic sector that such a change is necessary. To our reading, the implication of this part of Art 6(4) and recital 50 is that controllers should be able to conduct further processing where in accordance with law which safeguards important objectives of general public interest. However, we do not agree with a general provision which would leave it open to controllers to determine whether a relevant legal power exists to legitimate their further processing. This should be limited to a clear list of important objectives in the public interest which can be agreed upon as an acceptable list via parliamentary debate.

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?

Neither agree nor disagree

As an organisation, we are not aware of challenges justifying processing for a legitimate interest in the health and scientific or data sectors. However, it could be useful to provide a list of clear legitimate interests that will always outweigh the rights of data subjects if

these can be agreed. We are wary of this list being extensive as it is a powerful disapplication of data subject rights which could be used routinely and in different individual contexts if it is insufficiently specific.

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

Somewhat disagree

It is not clear that in all these cases the interest in processing will outweigh their impact on individual data subjects' rights. For example 'Improving the safety of a product or service that the organisation provides or delivers' and 'Using personal data for internal research and development purposes, or business innovation purposes aimed at improving services for customers' could be used very widely to process data for commercial purposes in ways that individuals would not expect or approve.

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

If a list is developed, one safeguard could be to enable the ICO to challenge an entry on the list and propose amendment or removal if it has evidence that it is leading to abuse of data subject rights.

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

Children's data requires particularly high protection and it is appropriate to maintain this safeguard.

Fairness in an AI context

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

Neither agree nor disagree

This question relates to areas of law outside the data protection regime. Different areas of law have different aims and purposes and these may justifiably give rise to different demands for developers. A lack of clarity about the requirements of any of these is unsurprising given the cutting edge nature of AI development and that it will inevitably take time for the appropriate application of the law to be agreed in relation to new developments. The response to this should be to seek to quickly and efficiently develop such applied interpretation of the law in authoritative guidance, as opposed to

removing the law as an 'obstacle' which risks removing the protection it affords for important rights and interests.

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

As we discussed in our research on Black Box Medicine and Transparency there is scope for interpretation of the correct application of the concept of fairness in this domain, including what form of transparency is fair and how this may be achieved. However, as we discuss in our research, this is also highly dependent on the precise context of an application and it is difficult to elucidate one single approach to all AI.

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

The key legislative regimes and regulators would include ICO for transparency requirements and the Equality and Human Rights Commission (Equality Act 2010) for equality and anti-discrimination requirements. In the healthcare context, NHS Digital and professional medical guidance and their regulators (GMC and UKNMC etc) would be relevant.

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 disagree

The development of an appropriate concept of outcome fairness in data protection law must take place drawing on the norms of data protection law (the importance of the protection of fundamental rights and freedoms). While it is important to assist developers navigate, as far as possible, complex legal terrain, it is inappropriate to expect that the boundaries of similar principles will be contiguous across different areas of law. This is because different legal regimes have different aims and purposes. It could be entirely appropriate for data protection law to fill a 'gap' in the wider legal framework governing fairness of outcomes from technological innovation in the same way it is appropriate for product liability law to set a higher level of protection for consumers than would otherwise apply under general contract law for example. There should be a teleological interpretation of different laws in relation to their fundamental aims and these may result in

entirely appropriate differences.

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?

Neither agree nor disagree

In the health context, the challenge of accessing data of sufficient quality to develop models and tools is far from new and we have not identified a reason that AI development deserves special focus above and beyond the range of more conventional big data approaches that are already widely used. Indeed, the heightened complexity and potential lack of transparency involved in some AI driven approaches deserves greater safeguards and regulatory scrutiny. As we have responded throughout this consultation, within our own field of health and biomedical research, we have reservations about permitting the use of personal data more 'freely' if this involves a weakening of the law. In our research, we conclude the law itself strikes an appropriate balance between facilitating flows of data and protecting individual rights and freedoms. The real challenges relate to differences in interpretation of the law among a myriad of data custodians and wider issues such as a lack of confidence among the public. We would support measures to address these challenges and enable the responsible use of personal data more freely but we would not support the removal of legal requirements which risks a considerable further loss of public trust and confidence.

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?

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

Somewhat disagree

As we have responded elsewhere in this consultation, there is a danger in developing a list of automatic 'legitimate interests' that removes safeguards in the form of a need to balance a legitimate interest with the impact on the rights and freedoms of the data subject. We are cautious about the development of a list of default overriding legitimate interests since this balance may be different in different contexts (i.e. depending on the sensitive nature of the data at hand, as may be the case in areas of health or genomic data).

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 agree

We agree that further clarification should be provided to developers about mechanisms that exist to enable appropriate and safeguarded processing of sensitive (special category) data for these purposes. In our research we have heard from developers that they find it challenging to navigate the data protection regime. However, if the proposal is to clarify this through legislative change as opposed to guidance and assistance for developers navigating the law, we are cautious as such changes require careful balancing with the potential impact on individual rights and freedoms.

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 agree

We agree that developing a new substantial interest condition for these purposes would be preferable to attempting to fit these purposes with existing schedule 1 conditions. However, we are cautious of this proposal. This is because we are unclear about the scope of the processing that such a provision would enable. It could be argued that such a provision would enable a large range of processing which is primarily aimed at developing a tool or model and while the proposed limits may be sensible in theory, the result of processing to 'detect and correct bias would certainly be fed into the general operation of a model and its potential commercialisation. For example, could a commercial developer claim that they are simply processing data to detect and correct bias but in practice their primary aim is to develop the commercial potential of their product. If so, this could undermine reasonable expectations of the data subject and risk undermining their confidence in the whole data governance system.

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

The proposed safeguards (i) ensuring the processing is strictly necessary for this purpose; (ii) data is explicitly collected for bias/discrimination mitigation and not for any other purpose; and (iii) appropriate safeguards to remove risks of secondary use, e.g. by specifying technical limitations on re-use, and the implementation of appropriate security and privacy preserving measures, are sensible. We agree that demonstrating necessity and proportionality of such processing are key. We would also advocate for oversight and

guidance to ensure that this condition does not become an easy and default ground for processing special category data for commercial and other purposes, albeit alongside legitimate purposes in terms of detecting and correcting bias.

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?

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'

Somewhat agree

We have carried out significant research in relation to these aspects of data protection law and how they interact with the requirement for transparency (www.phgfoundation.org/briefing/black-box-medicine-transparency) and whether/how they align with the development of AI-driven approaches in digital pathology (www.phgfoundation.org/research/assessing-ai-for-early-detection-of-oesophageal-cancer). We have found that the limits and scope of these provisions are unclear and we agree with the approach in this consultation of seeking further evidence rather than making proposals for legislative change. In particular, we have identified significant ambiguity about what constitutes a 'decision based on solely automated processing', determining when such a decision may have legal effects or 'similarly significant effects' and how the provision operates fundamentally- as a right to object or as a prohibition.

In relation to the benefits and risks of clarifying the limits and scope of 'solely automated processing', we think there is an interpretative aid in the existing WP29 guidance on what would or would not constitute meaningful human involvement. i.e. that human involvement cannot be a token gesture or performed by someone without the ability to truly critically appraise the results of the algorithm. Further clarifying this in guidance would be beneficial. However, we think there is a risk of not further clarifying what constitutes a 'decision' in this context, although this will be challenging. For example, in our research we have discussed whether the output of a model at different stages of analysis of a biological sample constitutes a decision or whether the 'overall' end result and diagnostic decision of such a model constitutes the relevant decision. This is unclear and differs depending

on professional view but has important implications as there may be human oversight of the 'end' output but not automatically of the intermediate stages.

In terms of the benefits and risks of clarifying the limits and scope of 'similarly significant effects', our research has found that this is unclear and would benefit from clarification, and perhaps in a legislative change to remove 'similarly' from the article. With this removed, it may be helpful to clarify in guidance a range of areas where there may be significant effects for the data subject, for example, in the health context setting examples of impacts not only on direct treatment and care but also on prioritisation or triaging decisions that may result from more 'administrative' tools.

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

No

At present we cannot identify better alternatives to developing guidance and assistance for data controllers and AI developers on this issue. Alternative options would include removing Art 22 entirely or restricting its operation, and/or, providing a right to object/obtain human involvement in AI-specific legislation instead of in the GDPR. However, at present it is not clear if AI specific legislation should or could be developed in the UK and it is sensible to consult on adjustment to Art 22.

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'?

Somewhat disagree

Determining how well 'future proofed' any aspect of the UK GDPR is in relation to AI is very challenging. However, we agree with Paul de Hert and Guillermo Lazcoz that some adjustments are called for. In particular, as automated processing becomes widespread, it is questionable whether such processing should be capable of being justified as 'necessary for entering into, or performance of, a contract between the data subject and a data controller'. The informational asymmetry between the parties and complexity of AI processing means that it is unlikely that individuals will be able to critique this justification easily and it is potentially open to abuse.

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?

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)

Strongly Disagree

We agree with Paul de Hert and Guillermo Lazcoz that it would be counterintuitive to eradicate Article 22 because the use of automated decision-making is/will increase. It plays a fundamental role in safeguarding against rights abuse and discrimination where the UK has a longstanding reputation and is still bound by international treaties protecting such rights.

Clarification is needed on whether its purpose is to prohibit solely automated decision-making or to enshrine a legally enforceable right for human intervention in those decisions that carry significant risk of rights enfringement and/ or discrimination.

Risk is a clear driving factor in other AI regulatory approaches, in both domestic regimes (medical devices consultation) and international approaches, such as the EU's AI Liability Regulations and the FDA's approach to regulating AI medical devices. Risk-based approaches would help clarify 'significant effects' by distinguishing systems that could adversely impact the rights and lives of data subjects from those that carry out processing tasks that do not factor into decisions about persons, because a human person makes the final decision and that human person has meaningfully taken into account whether such persons have been disproportionately impacted by the way in which their data was processed. Data Impact Assessments will likely play an important role in monitoring this.

We suggest the Government first clarify the purpose of Article 22 as right to human intervention, then clarify what types of data processing it applies to and finally regulate human behaviour and oversight to ensure 'meaningful consideration' as the basis of appropriate safeguards within an amended Article 22. Repealing Article 22 entirely, or deregulation and excessive derogations and exemptions may lead to loss of public trust in AI driven innovation and

consequently may prove counterproductive to the UK's position as a leader in developing responsible innovation.

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.

We agree that the data protection framework is a difficult fit for information that has been inferred about an individual. This is because such information is at the boundary of personal and non-personal data. Whether such data are 'personal data' or not will depend on the strength of the probability involved and obtaining consensus about this is very difficult. Some inferences may be made with sufficient certainty to constitute 'personal data'. In our field, this may apply to genetic data which are the results of 'imputation' or 'filling in the blanks between sequenced parts of a genome based on statistical inference.

However, because it may be argued that some inferences cannot constitute personal data because they are simply guesswork and insufficiently certain to relate to or identify an individual there is a risk that profiling activities, including those based on health profiles, will not be regulated in data protection law (no matter what attempt is made).

We agree with the consultation at paragraph 106, that an attempt to specifically regulate inferred data itself is 'counterproductive' because the harm does not arise from the data itself, but the manner in which it is processed. The intersection of automation and inferences suggests that profiling may be better regulated through law relating to automated processing, whether of personal or non-personal data.

We are unclear on the reference in paragraph 107 to article 13 transparency requirements when article 14 would govern personal data that have not been obtained from the data subject. This would address some of the transparency challenges raised there.

We agree with the suggestion that Article 15 may not provide for a right of access to mere inferences but we would be very cautious that this is not the case where such inferences are connected in some way (as they must be to be useful to the controller) to an individual. It may be beneficial for the ICO to address this topic. It has an analogy with the challenge of 'shared' genomic data which may be connected to multiple genetic relatives- it is our view that such data are personal data when they are connected to an individuals health records for example, as they must be to be used for their clinical care.

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).

In our view, there should be careful consideration of whether the UK should adopt a regulatory framework to address automated and AI driven processing (in a similar manner to the proposed EU Regulation). If this is not the case, a proportionate risk-based approach should be taken to the governance of such processing and this may include proportionate transparency requirements. For example, transparency should be heightened in healthcare automation. Such regulation may also legislate for group impacts and the processing of non-personal data.

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.

Although we have answered that we don't think the data protection framework is a good fit for regulating collective harms, because it would require a fundamental re-definition of the key regulatory object, 'personal data', we believe it is important to bolster some of its provisions as far as possible. For example, it is crucial that controllers do not avoid their obligations in relation to imputed or inferred data and therefore there should be efforts to address, through guidance, the scope of such data, particularly in high risk domains such as health.

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 disagree

We have conducted significant research on identification and genomic data and we have reconsidered the challenge of determining identifiability in our subsequent research on the GDPR and Genomic Data. Although we agree that the test for identifiability is a relative one and we make a number of recommendations (for example that there must be more than 'singling out' alone of an individual in a dataset for identification to occur) we found no evidence that placing the test for anonymisation or identifiability on a statutory footing would assist the challenge. Regardless whether the test is placed in a recital, in guidance or on the face of the statute, there would remain significant scope for debate about its proper application to data in a specific context. Moreover, it risks unnecessary divergence with EU

data protection in a way that could hamper international collaboration in important areas such as biomedical research. We have seen this challenge in the context of EU-US biomedical research collaborations where disagreement about the status of the data (whether they are 'personal' or anonymous) has hampered crucial research collaborations.

What should be the basis of formulating the text in legislation?

N/A legislation should not be amended.

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)?

We strongly agree with this position and discuss our reasons in our research. In essence this is a logical approach that has a foundation in case law.

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.

We believe that the Government should be promoting privacy-enhancing technology. The Government is now doing so in the health research domain, through a commitment to and promotion of Trusted Research Environments. The most important further commitment in our view should be through resourcing the ICO to continue to address this topic and update its guidance in accordance with the state of the art. If a state of the art approach can be taken by the regulator this could dramatically reduce the uncertainty and scope for disagreement on the part of controllers.

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?

The PHG Foundation welcomes the opportunity to comment on this consultation on reforms to the UK data protection regime. We are a health policy think tank with a focus on genomics and innovative health technologies, and over the last five years we have conducted significant research on the interaction between data protection law and genomic data in healthcare and research.

In 2017 we published the report Identification and genomic data and in 2020 we published a comprehensive report from our year long ICO-funded research on the impact of the GDPR on genomic data processing in healthcare and scientific research. In this research we conducted legal analysis, stakeholder interviews and convened an expert meeting of specialists in genomic data, health, research and data protection to identify the key impacts of the GDPR on genomic data processing. Alongside this we have also carried out significant

research on the development of AI tools in healthcare, including the extent to which the GDPR requires machine learning in the context of healthcare and research to be transparent, interpretable, or explainable. These resources are freely available on our website.

Drawing on this and subsequent research, we have responded to the consultation questions and uploaded our answers to the online platform. However, we would also like to make some general comments about potential reforms that cut across multiple aspects of the proposals and different sections of the consultation document.

The importance of a continued 'adequacy decision' for the UK

An overarching concern is that the proposals risk diverging sufficiently from the European Union's standards that the UK will be adjudged to offer a lower (and inadequate) level of protection for personal data. This would jeopardise free flows of data between the UK and the EU, which are crucial to scientific and genomic research in particular.

The UK does not need to maintain an exact copy of the EU GDPR but we are concerned that some of the proposals could be viewed as sufficiently divergent to impact on adequacy. For example, the proposal to adopt a statutory test for anonymisation could lead to a view that the UK regime has a fundamentally different scope of 'personal data' to the EU. If this is narrower, it will de facto be viewed as offering lower protection. In our research we identified a range of challenges that EU/EEA collaborators faced agreeing and authorising international transfers of data outside the EEA. These included different views about whether data are 'personal data' or not, causing significant harm to international research collaborations in certain cases. At present the UK is not suffering from the same level of friction but this is at stake if reforms are brought forward to adjust the framework without due regard for the impact on adequacy.

Evolution not revolution

Allied to this challenge, we advocate for a gradual process of adjustment to our data protection laws, based on broad and deep consultation with relevant sectors, to ensure that the proposals will not unnecessarily impact international flows of data and will not lead to unwarranted lowering of the level of protection afforded to fundamental data protection and privacy rights. It is difficult to do justice to the novel proposals within this consultation given its breadth and length. We hope that this consultation is a starting point for continuing engagement about what is being proposed, and not the final opportunity for comment, especially since our lack of comment does not reflect a lack of familiarity with the context or relevant law but because we do not have resources to give each aspect the consideration that it is due.

Improving data protection for research

We strongly welcome the focus of this consultation on the impact of data protection on scientific research processing. We think many of the barriers identified and a number of the suggestions in this area are sensible. However, we question the strength of some of the claims made about the role of law as a barrier in these proposals. In our research, we identified that uncertainty and complexity were the key and overarching challenges for researchers. However, we recognised that both of these are inevitable in the application of a comprehensive and sector-agnostic new law.

Our work highlights that the challenge is not the wording of the law (although there are undoubtedly aspects that could be better drafted) but rather the inevitable scope for argument about its proper application in a specific context, such as genomic research. To change the law would be unlikely to significantly alter the scope for that argument. We recommend that as much resource and effort as possible is put into developing specific guidance, in consultation with relevant industries and sectors to address these challenges, rather than changes to the legislation.

The importance of the ICOs role and specific guidance

In our research we found considerable approval for the ICO's track record in producing user friendly and sensible guidance. What is required is resources for this to be expanded and updated to address new challenges. An obvious area for continuing and updated ICO guidance is de-identification and technical approaches to privacy preservation. If the ICO can keep pace with the state of the art this will give greater confidence to data controllers and subjects about the measures put in place to reduce (but almost never eliminate) threats to privacy. We strongly refute the concept of a 'surfeit of guidance' in this regard. The ICO's position means that its guidance is more authoritative than the range of other guidance or technical documents that may be produced by non-regulatory bodies.

Innovation, trustworthiness and data governance

As a policy think-tank championing the role of innovation in improving population health we welcome the Government's ambition to support innovation, particularly in our field of health. However, we believe that the UK's record is and should continue to be as a world leader in safe, effective and ethical innovation. This requires proportionate regulation that ensures controllers, such as AI developers, act in ways that demonstrate their trustworthiness and maintain the support and confidence of the public. As we address in our latest research on changes to the regulation of confidential patient information during COVID-19, public trust and confidence is paramount. A loss of

confidence can critically harm health research in particular, or even faith in the healthcare system.

Data protection law is only part of this picture. Alongside other areas of law and governance, including the common law of confidentiality, consumer protection and professional negligence, the goal of any reforms should be to safeguard fundamental rights and freedoms while supporting ethical innovation. This extends to aspects that are largely outside the realm of data protection. Notably the governance of non-personal data, addressing the challenges of opaque or adaptive high-risk AI, and addressing group, as opposed to individual, impacts. If this is successful, law and regulation will play an important role in supporting, not hindering innovation.

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

Somewhat agree

The PHG Foundation has evaluated the potential utility of alternative transfer mechanisms in the report - GDPR and genomic data. The ability to share and process genetic and genomic data is critical for much medical research and for clinical genetics services more generally.

Around 17% of people have an inherited genetic condition. Many of these conditions are rare, with a handful of patients and families being affected across the world. Research investigating these genetic conditions heavily relies on sharing data internationally because of the rarity of such conditions. Data sharing is needed to interpret the pathogenicity of the genetic change, and to understand the clinical symptoms associated with this change. Consequently, proposals that aim to further facilitate international transfers of data are welcome as long as they still uphold the highest data protection and rights standards because excessive relaxation would undermine the UK's healthcare safety.

Proportionality and context are critical in assisting internationally collaborative healthcare researchers to navigate the regulatory quagmire. Our research has highlighted the importance of context in determining whether genetic and genomic data is identifying (see Identification and Genomic Data Report) and that treating all genetic and genomic data as inherently identifying is misguided. Guidance to clarify that not all genetic or genomic data is inherently identifying would help address overly cautious approaches to certain types of data that are hindering international data transfers. Our published report addresses the current barriers to international transfers of genetic and genomic data and associated clinical and phenotypic data.

What support or guidance would help organisations assess and

mitigate the risks in relation to international transfers of personal data under alternative transfer mechanisms, and how might that support be most appropriately provided?

Uncertainty over what constitutes a 'transfer' could be problematic for the genomics sector given the presence of methods such as query-based research. CJEU judgments such as Lindqvist (C-101/01), Schrems I, Google Spain (C-131/12), and Wirtshaftsakademie (C-210/16) are examples of where the definition of 'transfer' may have added further confusion through possible conflation with terms such as 'accessibility', 'transit' and 'disclosure'. In such circumstances, it would be helpful to know whether 'making data accessible' falls or does not fall within the definition of a 'transfer' as just one example. We would also caution against approaches that do not treat data 'transits' as data 'transfers' because of the risks of data skimming from international servers with more relaxed regulatory environments.

Data transfers to international organisations may be more difficult for health researchers than third country transfers in two respects: they raise conflict of law issues and the interpretation of the EU GDPR's 'essential equivalence' may be more difficult to establish. Further clarification on these may ease uncertainty for international organisations that are integral to genomic research and development.

A rubric explaining factors for consideration may also help guide data controllers on the best alternative transfer arrangement for their intended purposes. For example, data controllers who are seeking to share data with various third countries may more appropriately apply for an adequacy agreement, as the scale of the proposed transfer balances the time and resources needed to obtain an adequacy agreement. Those seeking smaller and less risky transfers would be better directed to contractual methods such as standard data clauses etc.

Our analysis suggests that the genomics community should explore a number of legal mechanisms for transfer. They should lobby for third country adequacy in their jurisdiction, craft codes of conduct and certification mechanisms to demonstrate general compliance with the GDPR, work toward developing these mechanisms to satisfy Article 46, and, if necessary, rely on a safeguard or derogation that fits their particular legal position. In short, controllers should pick the right mechanism for their situation but also work as a sector to develop sector-wide solutions to the challenge of international data transfers.

Guidance and support on the most proportionate arrangement would be best provided in the form of published guidance by regulatory bodies, as opposed to legislative amendment. The only exception being that a definition of 'transfer' would be best developed under legislative amendment because the problem lies in too many different

definitions by regulatory bodies.

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

Neither agree nor disagree

More information is needed to understand the risks and benefits of this in practice in order to comment. In theory, it sounds encouraging as unnecessary burdens should be removed. It would also be important to understand whether this would be a blanket exemption or only for certain transfers.

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

Neither agree nor disagree

This is a very interesting proposal which requires further consideration and careful work to ensure that it strikes a correct balance between greater freedom for international transfers (which would be welcomed in the context of genomic and scientific research) and ensuring sufficient protection for privacy and security of personal data. We agree that different approaches may be appropriate in different contexts. For example, in the context of biomedical research, significant safeguards including pseudonymisation, encryption and binding data transfer agreements will commonly be in place to protect and secure data.

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

This is likely to be an area where considered guidance from the ICO is required to ensure sufficient confidence on the part of data controllers, particularly those handling sensitive health data.

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

The EU GDPR creates a hierarchy of transfer mechanisms. Options for alternative data transfer mechanisms can only be utilised if previous options have been exhausted. We are concerned that reliance on international transfers that rely on protections provided for in another

country's legislation may contravene EU data adequacy requirements. Our research has also highlighted that it may be problematic to find sufficient assurance that the promised safeguards in another jurisdiction are in place, appropriate and enforced. This might need specialist knowledge of other jurisdictions as well as in-house expertise (in the form of a DPO) may well be necessary.

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

Neither agree nor disagree

This approach could enable greater flexibility and improved safeguarding by taking into account the nuances of different industries and data types. However, more information is needed on the scope of the power. What evidential criteria would be necessary for the Secretary of State to give a particular mechanism officially recognised status? Would the Department undertake their own impact assessments to assess the safety and strength of the proposed safeguard?

To what extent do you agree with the approach the government is considering to allow certifications to be provided by different approaches to accountability, including privacy management programmes?

In our work on the GDPR and genomic data, one of our key conclusions was that codes of practice and certification provided a potentially useful option for the sector. However certification schemes appear to be more limited in scope: those applying to a limited set of processing operations within a stable technical context are most likely to comply with the GDPR. It is not clear whether certifications adopting these new approaches will meet the standard of essential equivalence.

To what extent do you agree that allowing accreditation for non-UK bodies will provide advantages to UK-based organisations?

Somewhat agree.

Research collaborations enabling and supporting genomic research are typically international in nature. Accreditation for non-UK bodies could be useful for the sector in being able to formalise international data flows for these data, knowing that they satisfy relevant safeguards.

To what extent do you agree that the proposal described in paragraph 270 represents a proportionate increase in flexibility that will benefit UK organisations without unduly undermining data protection standards?

Neither agree nor disagree

While the restriction on repetitive use of the derogations is not derived from the GDPR but from the interpretation by the WP29, the position

that such derogations should not be the norm is a logical conclusion to the structure of Chapter V. However, it could be beneficial for the repetitive restriction to be removed from certain derogations (ie the important reasons of public interest) but only where there are barriers to other mechanisms and this is a last resort. For example, this could be important in rare cases of international research collaboration where alternative transfer mechanisms cannot apply and where it is clear that the scientific benefits are in the public interest.

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'?

Streamlining data flows through allowing private companies, organisations and individuals to rely on the body's lawful ground for processing could be beneficial. However, we have a number of concerns about this proposal. First, this provision could reduce transparency if the nature of the relationship between that 'private company, organisation or individual' was not made clear. Merely being 'asked' by a body suggests that this relationship could extend from a verbal agreement through to a contractual agreement that was in the public domain. Secondly, it would be important to ensure that any company, organisation or individual who relied on this provision, were contractually obliged to meet/address/honour any data subject rights potentially infringed by data processed under this exemption, so that the rights owed to data subjects were protected.

As our answers to the next question demonstrate, interpreting the scope of this power, i.e., who can reasonably be said to be 'processing data on behalf' of a public body could be problematic. Potentially the number of organisations and individuals eligible to rely on this provision could be very broad. Extending this definition too broadly runs significant risk of diluting its impact, particularly if it is perceived as a way for companies and individuals to evade responsibilities that safeguard the rights of data subjects. Ultimately, this could lead to perceptions that data controllers and processors are untrustworthy, undermining public trust.

The key to retaining trustworthiness is, in part, through rigorous clarity about how far these powers extend and transparency about how they are used. Empirical work on public views has highlighted broad support for data to be used for research but have also highlighted the importance of transparency in sustaining public trust.

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

If this provision were introduced, public bodies should be obliged to

publish details of any individual or company who relied on their lawful ground under Article 6(1)(e). There should be consideration whether this is already required under Articles 13 and 14 or whether they should be amended to add that the data subject should be informed where any company, organisation or person relies on another body's lawful ground under Article 6(1)(e).

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?

The recent COVID-19 pandemic is a good exemplar of a public health emergency, where resources, services and infrastructures had to be collated and deployed under intense time pressure. The Government adopted a number of measures to facilitate and optimise the use of data during the pandemic to support these services and initiatives and the PHG Foundation has analysed some of these in detail in order to feed into future policy development (funded by the NIHR Policy Research Programme).

We have recently completed a report exploring the impact of the Control of Patient Information Notices which suspended the usual safeguards for the use of confidential patient information for research as a response to the COVID-19 pandemic. The express purpose of these Notices was to facilitate sharing of confidential patient information for a COVID-19 purpose. In the most recent iteration of the Notices, these purposes were defined very broadly, potentially including all health and social care, as well as public health surveillance.

Our research has highlighted that this 'COVID-19 purpose' is potentially very broad and that as the pandemic has progressed, there is increasing concern that the public health emergency posed by the continuing pandemic no longer justifies continuance of these Notices as a legal basis for processing confidential patient information. Perpetuating these Notices (and the data processing, sharing and retention that these Notices facilitate) in the absence of public support that they are a proportionate and responsible measure has the potential to undermine public trust.

Other empirical work on public attitudes to the sharing of confidential patient data has similarly demonstrated broad support for the government's use of emergency powers during the pandemic but has called for increased transparency. University of Manchester Citizens' Jury reports.

Given that these Notices have had a significant effect in streamlining data flows and in increasing confidence about the legitimacy of

sharing data, we question the need for additional powers as proposed in this question.

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

A key operational challenge has been the difficulty of distinguishing between research activities and surveillance (justified under public health powers). Defining what constitutes 'an emergency' and what activities might be deemed 'necessary' would help to ensure that the use of such a power is proportionate.

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

The use of algorithms is already an important component of decision-making for public authorities, government departments and government contractors. The UK GDPR includes provisions and safeguards which enforce a level of transparency about when algorithms are used, and how they work (e.g., Articles 13 and 14 require that the data controller provides information to the data subject about the existence of automated processing and the logic involved (global explanation)). Article 22 provides for additional information to be given to data subjects for solely automated decisions having legal effects or significantly similar effects, and sets out safeguards required (e.g., having a human in the loop).

The provision of information (as required by these provisions) is necessary but not sufficient to generate public trust in the government's use of data. Similarly compulsory transparency reporting is necessary but not sufficient if government departments have not shown themselves to be trustworthy users of algorithms. Building trustworthiness involves many elements (some of which are addressed in ethical guidance from bodies such as the EU AI High Level Group on AI).

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

We consider that transparency is a key element in demonstrating trustworthiness but that this, in itself is not sufficient to generate trust. Additional elements include:

- Demonstrating that the algorithm has been developed in ways that ensure that it will robustly carry out the task it is assigned, without increasing inequalities or inequities
- This might involve selecting representative training data
- Developing the algorithm in ways that do not create (or recreate) bias

- Using tools to ensure that developers understand how the algorithm works (i.e. that it is safe and effective, and does not rely on spurious characteristics within the data). Our reports on Black Box Medicine and Transparency highlight some of the issues that are at stake.
- That the users of the systems incorporating algorithms are properly trained and supported and have sufficient resources

Consequently we have considerable reservations about the potential value of mandatory transparency reporting.

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?

We disagree with the principle that public authorities, government departments and government contractors using public data should have exemptions to any requirement for compulsory transparency reporting. In order to build trustworthiness, we believe that government departments should be subject to the same rules as other organisations.

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

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

In our research we have not identified any situations that relate to this but we are aware that this may be the case and we would advocate a cautious and robust approach to expansion of this list.

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'?

We agree that interpreting the difference between substantial public interest and public interest is sometimes extremely difficult, however we do not think that it will necessarily be useful to use granular legislative changes to provide greater clarity. This is because interpretation is likely to be heavily dependent on contextual issues, for which the more appropriate support will be sector specific

guidance including case studies and other practical material. However we think it could be helpful to create a high level definition of 'substantial public interest' as described below.

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

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

Somewhat agree

We support creating a high level definition of the term 'substantial public interest' that is sufficiently future proofed, that it can encompass future legislative, technological and policy change. However, we think any definition should not be exhaustive, and it should be made clear that interpretation will heavily rely on context in many cases.

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?

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

We suggest that trying to generate an exhaustive list of activities which are always deemed to be in the substantial public interest will inevitably fail, because the legislative and policy landscape is not static, and bodies, regulations and the barriers and incentives to processing data constantly change. Therefore, there should be scope to amend the list over time based on careful consideration and consultation.

To what extent do you agree that the ICO would benefit from a new statutory framework for its objectives and duties?

Somewhat disagree

There is already a comprehensive statutory framework for ICO as a supervisory authority within the UK GDPR. Creating an additional or alternate statutory framework dilutes this overarching purpose and undermines the potential role of the ICO as an effective, proportional and responsible regulator.

To what extent do you agree with the proposal to introduce an overarching objective for the ICO with two components that relate to upholding data rights and encouraging trustworthy and responsible date use respectively?

We disagree that such a framework should be introduced.

Are there any alternative elements that you propose are included in the ICO's overarching objective?

We disagree that such an objective should be introduced.

To what extent do you agree with the proposal to introduce a new duty for the ICO to have regard to economic growth and innovation when discharging its functions?

Strongly disagree

It is important that ICO discharges its duties in ways that take account of the wider technological environment, and that it has the expertise to assess the impact of these innovative technologies. The guidance it produces should take account of the importance of innovation in changing the landscape for data protection. However we strongly oppose the creation of a new duty for the ICO to have regard to economic growth and innovation when discharging its functions, as we believe that this dilutes its responsibility as a regulator. We believe that introducing this additional duty could, in turn, undermine public trust and confidence in ICO as a regulator, and in the trustworthiness of infrastructures, systems and processes more generally.

To what extent do you agree with the proposal to introduce a duty for the ICO to have regard to competition when discharging its functions?

Strongly disagree

Please see the answer to Q5.2.4a. We believe that introducing this additional duty could, in turn, undermine public trust and confidence in ICO as a regulator, and in the trustworthiness of infrastructures, systems and processes more generally.

To what extent do you agree with the proposal to give the Secretary of State the power to require the ICO to set up a panel of persons with expertise when developing codes of practice and complex or novel guidance?

Somewhat agree.

As a policy think-tank focused on the health sector, our work has

highlighted the potential impact of codes of practice and sector specific guidance. In our report on the GDPR and genomic data, we highlight the potential advantages of developing codes of practice on key areas such as international data transfers and de-identification. In this report we have highlighted the need for all stakeholders to be involved in developing codes of practice relating to genetic and genomic data. Co-development of codes of practice together with ICO, the regulator, would be the best way forward. Our report has been discussed by the British Society for Genetic Medicine and also brought to the attention of the European Society for Human Genetics (the professional groups supporting clinical genetics services and genetic and genomic researchers in the UK and in Europe).

Our work on the regulation of algorithms has highlighted similar challenges for some machine learning / AI applications. Although ICO requires relevant expertise in order to understand the potential risks and benefits of data processing for these applications, and the appropriate and proportionate safeguards that might be required, we do not support a deterministic approach that treats all genetic/genomic applications as posing risks.

However, there must not be political influence in the choice of persons involved on the panel.

Contact: intelligence@phgfoundation.org