JAAG Response to the UK Government consultation 'Data A New Direction' 17 November 2021

Contents

Chapter 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?
○ Neither agree nor disagree

Q1.2.1a. Please explain your answer, and provide supporting evidence where possible.
We need greater clarity about what 'bringing together research-specific provisions' might encompass. If the intention is merely to bring together in one place all the various elements of the UK GDPR/DPA 2018 that address research, we have no objection. Whilst we approve of the aim of clarifying what researchers need to do, we are concerned that 'consolidation' must not be used as a pretext for suppressing necessary provisions. We require further clarification before we can express support or disapproval.

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

Q1.2.2a. Please explain your answer, and provide supporting evidence where possible.
It is not clear why it is proposed to define the term 'scientific research', nor for which researchers this would clarify the situation. The focus of the consultation document is quite broad and often refers only to 'research'. It is unclear what the approach would be for research that is not deemed to be 'scientific'. It may be helpful to have different categories of research that are handled in different ways, but it is not clear why this would be better than the existing more generic focus that includes 'purpose of processing'. Moreover, for 'blue skies' scientific research, the ultimate benefits to society may not be known in advance. Similarly, for other types of research that provide a basis for economic activity, service improvement, etc., it may not be realised until much later how these might result in various types of harm to society and other unforeseen consequences. In addition, there are already context and sector-specific ethical guidelines on what researchers should do.
Therefore, making the most appropriate guidelines for a given context known to researchers would be an important aspect in clarifying what researchers should do. This would supplement the existing law rather than replace it.
Overall, JAAG finds that the case has not been made that the proposed approach will have the desired effect. For example, in the field of industrial safety, prescriptive definitions of terms triggered a proliferation of topic- specific regulations, which then had to be swept away because they were ineffective and caused confusion for industry and regulators.

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?
○ No

It is clear that Recital 159 of the UK GDPR is an interpretative example; it does not constitute a definition of scientific research and is therefore not a suitable basis for a statutory definition. We question the need for such a definition.

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

JAAG believes that greater clarification needs to be provided about the government's intention in terms of changes in relation to 'scientific research' versus 'research', and the justification for this. In any case, we are not convinced of the merit of this overall approach to changing the existing legislation in this way; it seems to be motivated by a longer-standing desire by certain parties to remove the need for informed consent when using big data for 'research' purposes: see, for example J.P.A. Ioannidis, "Informed Consent, Big Data, and the Oxymoron of Research That Is Not Research", The American Journal of Bioethics, 13(4), Taylor & Francis Group, 2013.

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?
○ Somewhat agree

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

Identifying a lawful ground for personal data processing for research processes may indeed create barriers for researchers, but this need not be a bad thing. Researchers need to justify the extent to which personal data processing is really necessary for their research, and consider how they might reduce harm and risk whilst still producing interesting research results, if the research is worth undertaking. Some research just should not be carried out, for ethical reasons

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

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

JAAG notes that not all research undertaken by universities is automatically in the public interest: researchers may be motivated by economic gain, promotion opportunities and so on. JAAG is therefore concerned that this may become a 'catch all' ground that is applied without researchers or their supervisors paying sufficient attention to how applicable it really is in a given context. In considering whether or not a task is in the public interest, due weight must be given to the summation of the harm caused to individuals, and their individual human rights and in each case an argument must be made to justify any conflicts, as at present.
Furthermore, interpreting "public interest" exposes the researcher to the temptation of confirmation bias. In the words of Francis Bacon already in the Seventeenth century, *"it is the peculiar and perpetual error of the human understanding to be more moved and excited by affirmatives than negatives, whereas it ought duly and regularly to be impartial; nay, in establishing any true axiom the negative instance is the most powerful."* This has been our experience in safety-related systems: rather than ask "why is this system safe?", we ask "why might this system be unsafe". Here, we must ask "why might this research be harmful?".
JAAG believes that focusing on public interest alone is highly questionable and will lead to avoidable harm in some cases.

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?
○ Somewhat disagree

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

Not all research is ethical or good for society. There are existing guidelines relating to ethical research practices in different contexts. The stronger ones provide a substantive basis for checking whether something is indeed ethical or not. Research Ethics Committees operate in Universities, Hospitals, and are a legal requirement for various kinds of research involving human participants e.g. clinical trials etc. Universities also incorporate ethics boards in checking whether research is appropriate or not. Decisions about whether research is appropriate are complex. If the legal framework is simplified, there is a risk that insufficient oversight could be given to whether research should proceed. The legal framework helps to support the appropriate and due consideration of whether or not to proceed with research, and for these most important matters not to be swept aside. If anything, this oversight needs to be strengthened.

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

'Research' is a very broad term here; it need not at all result in public good, or even if it does, that might involve other kinds of harm. There must be appropriate oversight by independent experts that the research is appropriate, and they must have the power to prevent it. For universities, this is likely to involve their ethics boards, (which may indeed cover most research using human subjects); but the means for achieving this oversight are less clear for other types of research organisations. It is very important that decisions are made reflecting the interests of ordinary citizens and not those of the profit motive: this seems unlikely to happen without legal protection which is a good (and widely deployable) extra barrier. JAAG therefore considers that creating a new legal ground for research carries very significant risk.

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 disagree

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

JAAG regrets that the question centres on benefit to researchers and not benefit to citizens.
Recital 33 of EU GDPR says that "data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. This consultation question Q1.2.8 does not provide that caveat, so JAAG views the proposal as an unwarranted degrading of the protection for citizens as embodied in EU Directive on GDPR.
There is significant risk in this proposal if subjects are not informed of what the broader research would be. For example an organisation could put forward an initial innocuous research purpose that a data subject would support, but later follow up with a more potentially controversial research project (which may be thought by the researcher to be compatible, but not necessarily by the data subject). While a data subject may agree to their data being used for one research initiative, further use may not match with their values and beliefs (for example, political or religious reasons).
JAAG believes that it should be made clear to data subjects in advance of data collection if the data is to be sold (or transferred in any way related to a financial benefit from their data to the collecting agency/organisation).
Furthermore, JAAG points out that much will depend on the context, including who might be doing the processing (or further processing), the (new) purposes of processing and how much choice and transparency is given to data subjects, in a usable and comprehensible way. There is therefore an

issue of trust: the decision of data subjects would be affected by the extent to which they trust these entities.

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?
○ Somewhat disagree

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

Again, JAAG regrets that the question centres on benefit to researchers and not benefit to citizens: even if researchers benefit, it may not always be good for society to allow this. JAAG also notes that the question gives no indication as to the number of future research occasions for which the data could be used. For example, the data could be used time and time again if it were put in a data set made generally available for researchers (such as for testing AI models). In this context the use of the data could grow exponentially. Some data subjects may find this unacceptable.
JAAG believes that If the further processing increases the risk of harm to the persons whose data is being used, then this should not be allowed. For example, when researching the efficacy of a particular set of antibiotics, if the extra processing revealed linkage to other personal information such as the identity of the clinic or practice where the antibiotics were prescribed.

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

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

This proposal appears to be unbalanced: “disproportionate effort” to the researcher is taken into account, while potential harm to the data subject is ignored; this is unacceptable. It is not clear what ‘disproportionate effort’ means and how this will be decided, checked, judged and penalised.
Many actions might fit into the category of ‘processing for a research process’, and this proposal therefore increases risk and raises issues around transparency to the data subject when giving consent, which could affect trust.

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

An additional safeguard would be a time limit on the use of the data, after which time the researcher must either delete it, or get renewed permission from the persons concerned. This would be similar to a non-disclosure agreement. Ways also need to be found to clarify to the data subject that, essentially, they are being asked to consent to a much wider scope of research including that by other organisations, potentially (if appropriate) including research for commercial gain; such clarifications are quite common in practice e.g. on consent forms.
There may also be a place for the researcher to be able to show that they have conformed with best practice in the domain in which they work. For example, in a given context this may involve healthcare-specific guidance as well as the best practices set out by the Foundation for Best Practices in Machine Learning.

1.3. Further Processing

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

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

JAAG regrets that questions in block 1.3 position themselves as seeking clarification, but are actually proposing a very significant extension of what is legally permissible compared to the current legal situation under GDPR.

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

JAAG regrets that this question raises, but the consultation does not answer, the question of what exactly is meant by 'safeguards an important public interest' and how that is to be judged and checked. If many individual interests are passed over, the summation of these in itself may be regarded as a public interest too, to counter the alternative public interest that is being claimed, yet it is unclear how, or if, individual interests will be taken into consideration.

Q1.3.2a. Please explain your answer and provide supporting evidence where possible, including on:
Q1.3.2a1. What risks and benefits you envisage
Q1.3.2a2. What limitations or safeguards should be considered

From a technical viewpoint there are clear benefits from aggregating data sets, enriching learning data, etc. From a societal point of view the risks are less evident, but nevertheless there. Just because it is hard to envisage precisely what risks there might be does not mean that risk is absent. Again, if we take safety-related systems as an example, any change (to requirements, design, or any aspect of the system), no matter how trivial, is subject to an impact assessment which considers all aspects of risk. Equally, further processing and modifications to the tools and components used should be considered as a change and be subject to an impact assessment. The results of such an assessment should be accessible to the data subject so that transparency is maintained.

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

Q1.3.3a. Please explain your answer and provide supporting evidence where possible, including on:
Q1.3.3a1. How you envisage clarifying when further processing can take place
Q1.3.3a2. How you envisage clarifying the distinction between further processing, and new processing
Q1.3.3a3. What risks and benefits you envisage
Q1.3.3a4. What limitations or safeguards should be considered

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

Q1.3.4a. Please explain your answer and provide supporting evidence where possible, including on:
Q1.3.4a1. How you envisage clarifying when further processing can take place
Q1.3.3a2. How you envisage clarifying the distinction between further processing, and new processing
Q1.3.4a3. What risks and benefits you envisage
Q1.3.4a4. What limitations or safeguards should be considered

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 disagree

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

JAAG is seriously concerned that this proposal might allow current or future governments to add new elements to the list that could further erode individual rights. Even at this stage, the proposed list includes 'Using personal data for internal research and development purposes, or business innovation purposes aimed at improving services for customers' which is, in our view, far too broad and would encompass too many types of business activity. Instead, JAAG proposes that the government retain the current system, which is much preferable because a balancing check is made and the decision has to be duly justified.

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 disagree

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

Several of the proposed activities are too generic to provide adequate protection for citizens. In particular, 'Using personal data for internal research and development purposes, or business innovation purposes aimed at improving services for customers' seems to be phrased in such a way as to be open to abuse.

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

JAAG strongly opposes this approach.

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

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

Children's data needs extra special care, as widely recognised.

1.5. AI and Machine Learning

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

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

JAAG considers that the current legal obligations with regards to fairness are clear when developing or deploying an AI system. GDPR was designed to be applicable to this type of technology as well as legacy technologies.

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

Q1.5.2a. Please explain your answer, and provide supporting evidence where possible.
Although fairness is a complex notion, there is a particular challenge with AI in order to ensure statistical parity across protected groups as well as to assign similar outcomes to individuals regardless of sensitive attributes. Mechanisms exist for designing and monitoring such fairness throughout AI product development and deployment: see for example the technical best practices set out by The Foundation for Best Practices in Machine Learning, v1, May 2021.
Therefore, JAAG believes that developers must show evidence of use of these best practices so that they can be audited independently.

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.

UK legislation enacting GDPR is the main legislation covering fairness in processing personal data, so this is the initial reference point on this topic. Since fairness is a key data protection principle, and the ICO is the UK regulator covering data protection, JAAG believes that the main regulator should be the ICO. Furthermore, the ICO, as with all regulators, must be genuinely independent: its reports should not be vetted by ministers, and its appointments should be genuinely independent rather than being arranged by a selection committee under government influence.

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

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

The concept of outcome fairness in the data protection regime already exists. Fair Information Principles have been in place for decades and are somewhat technology neutral. JAAG believes that any changes in legislation are likely to erode the protections put in place for citizens after the second World War, which were a post-war settlement aimed to ensure that the atrocities against human rights that happened in that war do not arise again in Europe. By enshrining protections in laws we try to prevent these rights being gradually eroded.

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 disagree

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

Experience so far makes us doubt the ability of researchers to anticipate potential harms. The reinforcement of negative attitudes towards race, women, etc. is well known, for example, see *Algorithms of Oppression - How Search Engines reinforce racism*. There are many examples of algorithmic discrimination. Loosening safeguards, as appears to be proposed here, will only lead to more such problems. Using 'personal data more freely' might encourage the development of systems from which very personal inferences might be drawn, to the distress of the people concerned. This, taken together with the proposed fee individuals pay before they can find out what data is held on them, is why JAAG considers this to be a very damaging and unwelcome proposal.

Q1.5.6. When developing and deploying AI, do you experience issues with identifying an initial lawful ground?
Q1.5.6a. Please explain your answer, and provide supporting evidence where possible.
Q1.5.7. When developing and deploying AI, do you experience issues with navigating re-use limitations in the current framework?
Q1.5.7a. Please explain your answer, and provide supporting evidence where possible.
Q1.5.8. When developing and deploying AI, do you experience issues with navigating relevant research provisions?
Q1.5.8a. Please explain your answer, and provide supporting evidence where possible.
Q1.5.9. When developing and deploying AI, do you experience issues in other areas that are not covered by the questions immediately above?
Q1.5.9a. Please explain your answer, and provide supporting evidence where possible.

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 disagree

JAAG finds the proposal dangerous because the mechanism to ensure that such personal data is only used only for bias monitoring, detection, and correction is not made explicit. A situation could easily be imagined in which a company could offshore personal data to a third party in a lax jurisdiction for the ostensible purpose of "bias detection". Once offshore, there would be no recourse, personal data could be sold anywhere. JAAG insists that strong safeguards are needed to prevent bias monitoring, etc. from being used as a pretext for the covert sharing of personal data.

Q1.5.10a. Please explain your answer, and provide supporting evidence where possible, including on:
Q1.5.10a1. The key benefits or risks you envisage
Q1.5.10a2. What you envisage the parameters of the processing activity should be

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

JAAG believes that the best way of ensuring legal clarity is to maintain all of the relevant provisions of the current UK GDPR.

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

JAAG is very concerned that this proposal, when put together with other relaxations in legislation being proposed by the government in this consultation, could open up significant new risks for citizens. JAAG wishes the government to ensure that this proposal does not permit the use of this sensitive personal data for other purposes. It must not be the case that sensitive information is gathered and used within AI training sets ostensibly for the purposes of tackling bias, but then shared more broadly and used for other purposes.

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

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

JAAG considers that this proposal opens up new risks for citizens and the consultation document does not convince us that the benefits outweigh the risks. The law currently requires controllers to identify an additional legal condition to make processing sensitive data lawful e.g. consent. If any new conditions are defined too broadly, they could be (mis)used in place of other safeguards, eroding the protections we currently have. The law could be changed to enforce the rule that the processing of all personal data places a responsibility on the processing entity to include bias detection themselves and not to subcontract it.

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

A key safeguard is to ensure that all data subjects can easily directly access their data at no charge, and, without hindrance, object directly to the data controller and appeal to ICO if there has been a breach of the subject's rights. The development and use of privacy enhancing technologies could also play a role in reducing privacy risks, but it would need to be a legal obligation to determine the most appropriate and feasible privacy-preserving techniques (including both decentralisation and cryptographic methods) and to use them. We agree with proposals (page 36 of the consultation document) for (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.

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 disagree

Q1.5.14a. Please explain your answer, and provide supporting evidence where possible, including on:
Q1.5.14a1. The benefits and risks of clarifying the limits and scope of 'solely automated processing
Q1.5.14a2. The benefits and risks of clarifying the limits and scope of 'similarly significant effects'

We note that the All-Party Parliamentary Group on the Future of Work has said, in their report published 11 November 2021 that: "... the rise of remote working has increased public concern about the impact of remote monitoring and management. A core source of anxiety is a pronounced sense of unfairness and lack of agency around automated decisions that determine access or fundamental aspects of work. Workers do not understand how personal, and potentially sensitive, information is used to make decisions about the work that they do; and there is a marked absence of available routes to challenge or seek redress. Low levels of trust in the ability of AI technologies to make or support decisions about work and workers follow from this. We find that there are even lower levels of confidence in the ability to hold the designer, developers, and users of algorithmic systems meaningfully accountable for their responsible governance".

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

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

JAAG considers that the best alternative is to keep the existing legislation, which serves an important purpose. Automated processing can give rise to injustice in a number of ways, even some that the designer or programmer did not envisage at all. It can affect important elements of social justice that were previously left to the market, state and society. It is increasingly being used for sorting citizens into social hierarchies of status and esteem and may give rise to new forms of 'digital disrespect' and exclusion.
In order for a data-based algorithm to be *just*, the data should be demonstrably well selected, complete, up to date and devoid of selection bias. Rule- based injustice can be due not only to overtly unjust rules but also to implicitly unjust rules - that for example indirectly treat some groups more favourably than others - or even neutral rules. Computer scientists may think that if an algorithm is *neutral* then it must be just, but this is not true - in some cases, treating disadvantaged groups the same as everyone else might entrench injustice. As Desmond Tutu said, a mouse with an elephant standing on his tail does not appreciate the elephant's claim of neutrality. The way forward is that humans need to monitor and prevent algorithmic injustice. Therefore, making processing solely automated, excluding humans from the loop altogether, is a step in the wrong direction. Inevitably this can lead to a variety of inhumane, clinical, uncaring and damaging situations.

1.5.16. 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

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

There are other parts of GDPR covering requirements for partially automated decision making and profiling, etc. These protections, including Article 22, are extremely important to keep.
Problems caused when partially automated decision making goes wrong are numerous. For example:

1 A UK passport photo checker shows bias against dark-skinned women (Source www.bbc.co.uk · 2020). Women with darker skin are more than twice as likely to be told their photos fail UK passport rules when they submit them online than lighter-skinned men. BBC research found this check to be less accurate on darker-skinned people. More than 1,000 photographs of politicians from across the world were fed into the online checker. The results indicated: Dark-skinned women are told their photos are poor quality 22% of the time, while the figure for light-skinned women is 14%; Dark-skinned men are told their photos are poor quality 15% of the time, while the figure for light-skinned men is 9%; Photos of women with the darkest skin were four times more likely to be graded poor quality, than women with the lightest skin.

2 IBM's "Watson for Oncology" Cancelled After $62 million and Unsafe Treatment Recommendations. In 2013, IBM partnered with The University of Texas MD Anderson Cancer Centre to develop a new "Oncology Expert Advisor" system. IBM's role was to enable clinicians to "uncover valuable insights from the cancer centre's rich patient and research databases." In July 2018, StatNews reviewed internal IBM documents and found that IBM's Watson was making erroneous, downright dangerous cancer treatment advice. In one case, Watson suggested that doctors give a cancer patient with severe bleeding a drug that could worsen the bleeding.

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 disagree

Q1.5.17a. Please explain your answer, and provide supporting evidence where possible, including:
The European Consumer agency recommends in their analysis 'Automated Decision Making and Artificial Intelligence: A Consumer Perspective' (June 2018) beuc-x-2018-058_automated_decision_making_and_artificial_intelligence.pdf that there should be the rights to object to automated decision making and to contest the decision of automated decision making; furthermore, users should have a right to transparency on which parameters offers are based and how the machine has arrived at its result. AI products must be designed so as to avoid undue discrimination, invasive marketing, or loss of privacy. We agree with this. JAAG considers that the combination of this and the other proposals will lead to increasing harm to, and lack of control and transparency for, citizens. The Government's proposal seeks to reduce legal safeguards, for example, processing based on 'legitimate interest' potentially covers a broad range of operations. We provide some examples below illustrating ways in which unfortunate situations may result in this and similar cases.

We list here some artificial intelligence and automated decision-making examples arising recently in the UK alone.

- In June 2020, four working single mothers successfully defeated a court appeal by the Department of Work and Pensions following considerable hardship to them due to loss of Universal Credit income arising from a design failure (related to pay date clashes) within the automated system used in Universal Credit and the refusal to fix this.
- Last summer the exam regulator Ofqual downgraded almost 40% of the A-level grades assessed by teachers, which culminated in a government U-turn and the system being scrapped.
- We have received first-hand evidence from a recent victim of a catalogue of spiralling, inter-related credit problems which began with one poorly designed credit check. This claimed that he was "credit unworthy" despite the fact that Experian had always shown his credit score to be

"fantastic". It ultimately led to his bank account being closed because of suspicions of money-laundering, his credit card being refused credit despite him always paying off his debts at month end, mobile phone and streaming contracts being refused, and many more; all of these stem from him being given a negative 'tag' by an automated algorithm.

- The owner of a Tesla Model S car was caught on camera using his car's self-driving Autopilot function while sitting in the passenger seat, while travelling at speed on the M1 motorway, says he is "the unlucky one who got caught" implying that other Tesla drivers drive like this. In the UK the driver is required by law to remain in control of the vehicle at all times and must keep hands on the steering wheel. Tesla's Autopilot system does not give cars fully autonomous, self-driving capabilities.
- The CEO of a UK-based energy firm received a call from his German boss instructing him to transfer €220,000 ($243,000) to a Hungarian supplier. The 'boss' said the request was urgent and directed the UK CEO to transfer the money promptly. Unfortunately, the boss was a 'deep fake' voice generation software that accurately imitated the voice of the real human. It used machine learning to become indistinguishable from the original, including the *"slight German accent and the melody of his voice,"* as reported in The Wall Street Journal (https://www.immuniweb.com/blog/top-10-failures-of-ai.html)
- Amazon has stopped using their AI tool for Recruitment because their engineers trained it to be Misogynistic. engineers realized that they'd taught their own AI that male candidates were automatically better.

Q1.5.17a1. 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.

We have given examples in answer 1.5.16 of situations that can arise from solely automated decision making. Further examples from the US of harms caused by algorithmic decision-making in the high-stakes spheres (for individuals) of employment, credit, health care and housing are given in R.K. Slaughter, "Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission", ISP Digital Future Whitepaper, August 2021. This documents the dangerous potential for algorithms to amplify injustice whilst at the same time making injustice less detectable. To summarise, on p58: "Developers create algorithms with faulty inputs and flawed conclusions. They fail to test their models and rely on proxies that foster and often exacerbate discrimination. They create powerful engines that monetize attention, surveil consumers, and manipulate behavior without regard for the societal consequences. Their deployment of algorithms also imperils competition. If left unaddressed, these algorithmic flaws will repeatedly and systematically harm consumers."

Q1.5.17a2. 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)

JAAG believes that it is vital to ensure that the decision given by the system is fully transparent and understandable for the person(s) affected, that they have the right to review the decision outcome with a human being, and have full rights to redress. The young, and vulnerable people in particular would be at risk.
JAAG agrees with the viewpoint of R.K. Slaughter, "Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission", ISP Digital Future Whitepaper, August 2021 that "There also may be certain applications of AI and algorithms that pose such a profound risk of injustice to vital life functions or opportunities that a moratorium might be appropriate and necessary."

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

When considering the effectiveness and proportionality of data protection tools, provisions, and definitions to address profiling issues and their impact on specific groups, some key issues emerge. These relate to whether it is appropriate to collect, store and draw inferences from specific characteristics or attributes, and what limits there are on how they might be used to affect the individual (including in a discriminatory way). Knowledge of certain data, and the way that it is shared, can itself be an issue, especially where sensitive information is involved. For example, information about political opinions and personal health is not information that - either directly or indirectly via inference - many citizens would like to be collected and shared. The risk of harm in doing so is high. We are not convinced that it is a good idea for detailed profiles to be built up around individuals. Neither for individuals to be matched against certain types of information to predict other kinds of behaviour or opinions that may be sensitive. Key mechanisms for addressing this issue include both legislative restrictions based on ethics and human rights, as at present, and impact assessments. Impact assessments may not be unified, but they are context- dependent so it is not always appropriate that they are unified, nor is it necessary since each focuses on a different domain; it would not be too difficult to ascertain which might be appropriate for a given context. The other initiatives cited in paragraph 111 are also useful as background. If the government mandated more, and the regulators were better resourced and could make use of stronger penalties, companies would be encouraged to devote more attention to addressing such issues.

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

For privacy and security reasons it is not always appropriate to share data, if this contains sensitive or personal information, so the context here is key; however, it may be that meta-level properties and actions could still be shared. Transparency in some circumstances could be to independent accredited authorities who carry out detailed, ethical auditing and who are able to share the findings. Where possible, public registers would be useful: the city of Amsterdam has started a register of artificial intelligence systems and algorithms used by the city authorities that can be inspected by the public and which demonstrates their ethical and social justice credentials. One of these, for example, calculates the probability of an illegal holiday rental situation, triggered by a report of possible fraud. A Data Protection Impact Assessment (DPIA) is one form of verification for accountability that should be used in conjunction with others. It can be used to help provide transparency about the nature of the risks, including the criteria used in the risk assessment, how decisions are made to mitigate risk, and whether the mechanisms to be used and implemented are appropriate for the context. It follows that legislation to mandate and encourage this should be maintained. Comprehensive obligations for controllers to inform supervisory authorities and data subjects of personal data breaches further increase transparency and should be encouraged. It is not only customers and end users that might be affected by certain kinds of data processing, but society at large. Transparency should therefore also be aimed at the general public and the regulator. This contributes to the maintenance of ethical standards, rather than stimulating a race to the bottom (of cost and privacy protection).

Q1.5.20. Please share your views on whether data protection is the right legislative framework to evaluate collective data-driven harms for a specific AI use case, including detail on which tools and/or

provisions could be bolstered in the data protection framework, or which other legislative frameworks are more appropriate.

Data protection is the right baseline to evaluate collective data-driven harms to individual citizens, since that is part of its remit. In certain domains, supplementary legislation may be necessary. This is similar to domain-specific ethical guidelines, giving greater information about specific contexts without invalidating the more general frameworks.
At the heart of data protection there is more than protection of the data – there is protection of the person to whom the data relates. Transparency and accountability disclose satisfactory (or unsatisfactory) stewardship of data which to the originator – either Data Subject or Data Controller – is not just data but is information that has a value, either (for the Data Subject) in terms of potential harm or possible benefit or (for the Data Controller) through its business value or in costs incurred in collection and processing.

1.6. Data Minimisation and Anonymisation

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

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

Guidance should change in line with technological changes and advances in mechanisms for more effective anonymisation.

Q1.6.2. What should be the basis of formulating the text in legislation?
○ N/A - legislation should not be amended

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

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

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

The data may be identifiable in another party's hands (either someone with whom the controller has shared the information or an attacker). With vast amounts of computing resource now increasingly available, and depending on the anonymisation technology used, many anonymisations can be reversed. This means that great care needs to be taken to protect this information, especially as it may be abused in the future either by being shared or by technological advances (more powerful means of reversing anonymisation) making this even easier.

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.

JAAG emphasises that it should! Yes, incentives should be created for its use, across a wide range of domains. In some circumstances, it should be a requirement to use these techniques as a prerequisite to engaging in the activity. It should generally be part of best practice across a product

or service lifecycle to determine the most appropriate and feasible privacy-preserving techniques, including analysis of the appropriateness of decentralisation and cryptographic methods; this is already part of privacy by design methodology and is included within context-specific frameworks including that proposed by The Foundation for Best Practices in Machine Learning. There are many different techniques for improved anonymisation, e.g. differential privacy techniques, k-anonymity, l-diversity, etc. and these should be encouraged: depending on the techniques used, greater facility for organisations to operate on sensitive datasets etc. could be given. This is analogous to safety-related applications where methods of greater rigour are required for higher levels of integrity.

1.7. Innovative Data Sharing Solutions

Q1.7.1. Do you think the Government should have a role enabling the activity of responsible data intermediaries?
○ No

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

JAAG considers that enabling the activity of responsible data intermediaries can be done already under the existing framework. What is proposed undermines the role of the consent of data subjects in having choice, control and knowledge about how information, including very sensitive personal information is used and shared around. The proposals risk encouraging abuse and reducing transparency for data subjects, with information being used in ways that citizens would find harmful and objectionable.

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

Consent should be the main grounds used. Transparency and allowing the revocation of consent are also very important - the use of other grounds to legitimise intermediary activities opens up potential risks. There are other legal grounds such as contracts or acting on legitimate interests that could be used for intermediaries. However, to mitigate potential risk, these must be used with the right safeguards such as the right to object, balancing tests, tightly worded contracts etc. In addition, it would need to be clear if the intermediary is a processor or a controller, and that they comply with their respective legal responsibilities.

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

Q1.7.2a1. If Article 6(1)(f) is relevant, i) what types of data intermediary activities might constitute a legitimate interest and how is the balancing test met and ii) what types of intermediary activity would not constitute a legitimate interest

The types of data intermediary activities considered as a legitimate interest should be severely restricted. It should only be allowed for a small number of cases where the activity is clearly in the public good, and, it would be impossible to ask for consent. Part of the balancing test should be that privacy- enhancing technologies must be used where possible to minimise the risk to individuals.

Moreover, intermediaries must be actively transparent to the data subjects about what they are doing with citizens' data, so that data subjects are kept informed, and means should be provided for strong oversight, remediation and redress.

Q1.7.2a2. What role the Government should take in codifying this activity, including any additional conditions that might be placed on certain kinds of data intermediaries to bring them within scope of legitimate interest

JAAG believes that the existing structure based upon consent is preferable to trying to bring more kinds of data intermediaries within the scope of legitimate interest. This proposal, combined with certain other proposals being made in the document, could result in data intermediaries being given too free a rein. This would lead to citizens' data and other sensitive data being traded and used in ways that are not very transparent, and without citizens being able to control, or object to this.

Q1.7.2a3. Whether you consider a government approved accreditation scheme for intermediaries would be useful

JAAG believes that a government approved accreditation scheme might be useful to raise standards, but it should not mean that those accredited intermediaries are no longer required to justify all their activities in terms of public good. Many intermediaries will not be primarily motivated by public good but rather by the profit motive. Any accreditation must entail regular surveillance and audit of the accredited intermediaries.

1.8. Further Questions

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

Potentially, all of these could impact on such people. It would be particularly concerning that peoples' choice and control over the collection and use of their sensitive information would be reduced. For instance, decisions might be made about them without a human in the loop to explain and check issues, their information would be shared and used much more widely, and there could be increased risk that there would be more information gathered about them that could be de-anonymised. Their life could move towards one of increased surveillance and potential discrimination without knowledge or redress. JAAG considers the probability and severity of these impacts being negative is higher than them being positive.

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

Q1.8.2a. End of chapter Q. Do you have any general comments about this chapter not yet captured by your responses to the questions above?

We appreciate that new technologies open up new opportunities, many of which may benefit society. However, we are concerned by the way in which the proposed reforms would together shift our society in the wrong direction. Where many different parties constantly monitor and build intrusive profiles about citizens, which are then used in diverse ways not apparent to or controllable

by the data subjects themselves. Citizens are becoming the entities being bought and sold, and it is increasingly difficult to opt out of this. This has elements of a dystopian future to which the public has not acquiesced, and runs very much counter to Enlightenment values and the post-WW2 Western human rights settlement. Human values and culture do not change as quickly as technology. JAAG strongly believes that society needs to find ways forward that put the public good and our core values at the heart of decisions about what to allow in terms of new, risky business opportunities. These proposals do not yet seem to be pointing in the right direction.

Chapter 2 Reducing burdens on businesses, delivering better outcomes for people

2.2. Reform of the Accountability Framework

Q2.2.1. To what extent do you agree with the following statement: 'The accountability framework as set out in current legislation should i) feature fewer prescriptive requirements, ii) be more flexible, and iii) be more risk-based'?
○ Somewhat disagree

Q2.2.1a. Please explain your answer, and provide supporting evidence where possible.

Enhancing accountability can be an improved basis for trustworthiness. Higher degrees of accountability, if appropriately advertised, could result in higher acceptance and trust by prospective customers so is good for business. In order to be adopted, accountability must deliver effective solutions whilst avoiding where possible overly prescriptive or burdensome requirements. On the other hand, accountability can also be used as a smokescreen for decreasing individual rights and for allowing businesses to chase profits without due regard to the wider effect on society. The concept of 'strong accountability' is very important in helping demonstrate why (and indeed whether) an organisation should be trusted as well as in preventing the latter. (cf. Strong Accountability and Its Contribution to Trustworthy Data Handling in the Information Society | SpringerLink i.e. Pearson S. (2017) Strong Accountability and Its Contribution to Trustworthy Data Handling in the Information Society. In: Steghöfer JP., Esfandiari B. (eds) Trust Management XI. IFIPTM 2017. IFIP Advances in Information and Communication Technology, vol 505. Springer, Cham. https://doi.org/10.1007/978-3-319-59171-1_15)

Q2.2.2. To what extent do you agree with the following statement: 'Organisations will benefit from being required to develop and implement a risk-based privacy management programme'?
○ Somewhat agree

Q2.2.2a. Please explain your answer, and provide supporting evidence where possible and in particular:

We note that with OECD guidelines as mentioned in the proposal, GDPR etc, accountability is generally related to the responsibility of the data controller (in respect of its legal requirements for treatment of personal data) and to adequate remediation and redress when things have gone wrong; as such, it does not replace privacy requirements but rather is complementary and integral to those requirements. In this context, developing a risk-based privacy management programme can be part of an effective solution for data protection that reflects the context of business operation and builds in mechanisms and processes for enacting at least the legal minimum of privacy requirements and ideally a higher base motivated by ethical values.

Q2.2.2a1. Whether a privacy management programme would help organisations to implement better, and more effective, privacy management processes.

Yes, an organisational privacy management programme should help to implement better, and more effective, privacy management processes. However, it is not necessarily the case that the organisational privacy management programme should be risk-based and in many cases this would itself create new risks. Particularly, that citizens' rights would not be taken sufficiently into consideration and that democratic accountability would be reduced. Any such system needs to be

developed to counter such risks: hence there is a need for strong accountability (see below), including adequate resourcing of non-colluding parties holding such organisations to account, if such systems are to be used.

Q2.2.2a2. Whether the privacy management programme requirement would risk creating additional burdens on organisations and, if so, how.

It requires significant effort to run a privacy management programme properly, and must be proportionate to the size of the organisations and the potential risk. For example, the requirements for a small charity differ from those of a large tech company. Also, a small business engaging in risky behaviour must do the appropriate risk assessment prior to the relevant project. Whether this would create an additional burden would rather depend upon how attentive to compliance and ethical aspects an organisation was before doing this, and whether the requirements suddenly change. For example, if an organisation does not pay proper consideration to data subject request requirements and just deals with these by hand, they may find that the burden of compliance would increase suddenly if an influx of requests come in. On the other hand, if they had planned and installed a suitable procedure for handling such requests they would not be overwhelmed. Overall it is rather like security management: selection of appropriate controls for the context should be the most appropriate way forward. Here, the context will depend upon the regulatory requirements of the domain and countries in which the organisation operates, as well as its ethical stance.

Q2.2.3. To what extent do you agree with the following statement: 'Individuals (i.e. data subjects) will benefit from organisations being required to implement a risk-based privacy management programme'?
○ Somewhat disagree

Q2.2.3a. Please explain your choice, and provide supporting evidence where possible.

It is not necessarily the case that data subjects will benefit from organisations being required to implement a risk-based privacy management programme. On the one hand, it is definitely a good thing that organisations do properly consider and adequately mitigate privacy risks within the context in which they operate, and explain and justify what they have done to others, including the public and independent regulators. On the other hand, it will not be a good step forward for individuals if organisations no longer have to take account of data subjects' viewpoints about the use of their data or offer them control over what happens to it. Individuals may lose informational self-determination and come under greater surveillance without their knowledge or consent. The concern is that any organisational assessment of an individual's data protection risk is not likely to rate that particularly highly, especially if not aggregated or with longer term effects not taken into account. The two (i.e. risk-based privacy management programme and abandonment of core individual data protection rights) do not at all need to be linked. However, from the given proposals it seems that the government wishes to offer the first to citizens in compensation for them losing the second. Citizens should have both.

Q2.2.3a1. Please share your views on which, if any, elements of a privacy management programme should be published in order to aid transparency.

Accountability should have democratic and ethical characteristics, in which transparency should be as high as possible in relation to other interests. Regulatory and supervisory authorities should have a primary role in the verification of the level of organisational compliance. One important aspect which needs to be clarified is how exactly the risk is being assessed: it is notoriously difficult to measure

harm to individuals, especially if the risk concerns breaches of online human rights. Many aspects of this need to be subject to public scrutiny: the standards and models that are being used, and how comprehensively privacy is covered within these; how the financial value of individual harms are allocated in a model; how future harms are discounted over time; whether harms to individuals are summed and the summation considered. Furthermore, it would often be appropriate to make public information about non-compliance and data breaches.
JAAG believes that transparency should be increased, in ways that do not decrease privacy or security. This includes the nature of accounts being public where possible, and the need for the responsibilities of the data controller to be properly understood by the data subjects (and other parties). For example, not buried in long and unreadable privacy policies.
In addition, the mechanisms used and relevant properties of the service providers in the provision chain need to be clarified as appropriate to customers and regulators.

With other measures, Data Protection Impact Assessments (DPIAs) and Privacy Impact Assessments (PIAs) are a form of verification for accountability that should be used to help provide transparency about the nature of the risks, including the criteria used in the risk assessment, how decisions are made to mitigate risk, and whether the mechanisms to be used and implemented are appropriate for the context.

Comprehensive obligations for controllers to inform supervisory authorities and data subjects of personal data breaches in a timely manner would further increase transparency.

It is not only customers and end users that might be affected by certain kinds of data processing, but society at large. Transparency should therefore also be aimed at the general public and the regulator. This contributes to the maintenance of ethical standards. Rather than stimulating a race to the bottom (of cost and privacy protection), it seeks to encourage an ascending spiral of improved privacy and protection. Such improvements have already been achieved in some fields of functional safety and environmental protection.

Q2.2.3a1. What incentives or sanctions, if any, you consider would be necessary to ensure that privacy management programmes work effectively in practice.

In order to strengthen the link between accountability and trust by providing stronger grounds for trustworthiness, we argue for the notion of *strong accountability*, which encourages ethical characteristics (such as high transparency in balance with other interests) and trustworthy mechanisms for producing and verifying logs as well as adequate enforcement. We believe that an accountability-based approach should have the following characteristics, which together support a strong accountability approach:

- *Support for externally agreed data protection approach:*
  Accountability should be viewed as a means to an end (i.e. that organisations should be accountable for the personal and confidential information that they collect, store, process and disseminate), not as an alternative to reframing basic privacy principles or legal requirements. In this way, the accountability elements proposed within GDPR are instrumental to provide a certain assurance of compliance with the data protection principles, but do not replace them. DPIAs, codes of conduct and certifications are proposed to increase trust in service providers who adhere to them.
- *Clarity of responsibility*:
  The commitments of the data controller need to be well defined – this is (part of) the aspect of responsibility, that is an element of accountability. Service provider responsibilities should be defined in contracts. The definition of standard clauses by the industry, as validated by regulators,

will help service users (such as cloud customers) with lower negotiation capabilities. The commitments of the data controller should include all applicable legal obligations, together with any industry standards (forming part of the external criteria against which the organisation's policies are defined), as well as any other commitment made by the data controller in privacy statements. In the cloud context, this is particularly important as entities may have multiple roles, e.g. they could be a joint controller and processor. Once again, the responsibilities of the entities along the service provision chain need to be clearly defined, including relative security responsibilities. On the other hand, certain tasks will need to be jointly carried out to be effective, such as risk assessment and security management. In this case there is a clear need for cooperation and coordination.

- *Transparency:*
  JAAG believes that transparency should be increased, in ways that do not decrease privacy or security. This includes the nature of accounts being public where possible, and the need for the responsibilities of the data controller to be properly understood by the data subjects (and other parties).
- *Trustworthy mechanisms for producing accountability evidence:*
  Trustworthy evidence needs to be produced and reflected in the account, for example, by using automated evidence acquisition and secure storage of instances of non-compliance. Accountability evidence needs to be provided at a number of layers. At the organisational policies level, this would involve provision of evidence that the policies are appropriate for the context, which is typically what is done when privacy seals are issued. But this alone is rather weak; in addition, evidence can be provided about the measures, mechanisms and controls that are deployed and their configuration, to show that these are appropriate for the context. For higher risk situations, continuous monitoring may be needed to provide evidence that what is claimed in the policies is actually being met in practice. Even if this is not sophisticated, some form of checking of the operational running and feeding this back into an organisation's accountability management program in order to improve it is part of accountability practice.
- *Protection of evidence, assessments and accounts against tampering:*
  Technical security measures (such as open strong cryptography) can help prevent falsification of logs. Privacy-enhancing techniques and adequate access control should be used to protect personal information in logs together with other accountability evidence. Note, however, that data that is collected for accountability might be itself data that can be abused, hence it also needs to be protected. The potential conflict of accountability with privacy is somewhat reduced as the focus in data protection is not on the accountability of data subjects but rather of data controllers, who need to be accountable towards data subjects and trusted parties such as the supervisory authorities.
- *Verifiability:*
  This is the extent to which it is possible to assess norm compliance. Accounts must be adequately verified and collusion between the accountor, its partners and the accountee must be prevented. There needs to be a strong enough verification process to show the extent to which commitments have been fulfilled. Audits should be regular, in a similar way to Sarbanes-Oxley external audit, rather than one-off checks at the accountability programme level. Note however that missing evidence can pose a problem, and guarantees are needed about the integrity and authenticity of evidence supporting this verification and the account. In addition, the actor carrying out the verification checks needs to be trusted by the data subject and to have the appropriate authority and resources to carry out spot checking and other ways of asking organisations to demonstrate accounts. That is why the data protection authorities play a key role in trust verification, for example in data protection certification. There are further aspects supporting this approach in terms of responsibility and transparency, as listed above. In terms of external governance mechanisms, strong enforcement strategies, not only in terms of verification, but also in terms of increasing the likelihood of detection of unlawful practices and strong penalties if caught, are a necessary part of accountability.

Q2.2.4. To what extent do you agree with the following statement: 'Under the current legislation, organisations are able to appoint a suitably independent data protection officer'?
○ Somewhat agree

Q2.2.4a. Please explain your choice, and provide supporting evidence where possible.

The data protection officer should ideally come from outside the organisation, however this depends on the organisation's size and resources. If they are an employee, they should be given appropriate training and sufficient independence to carry out their role effectively. Training is provided by organisations such as IAPP, and appropriate qualifications may be obtained with just a few weeks' study, thus making a shortage of supply fairly quickly self-correcting.

Q2.2.5. To what extent do you agree with the proposal to remove the existing requirement to designate a data protection officer?
○ Strongly disagree

Q2.2.5a. Please explain your answer, and provide supporting evidence where possible.

JAAG strongly believes that accounts must be adequately verified and collusion between the accountor, its partners and the accountee must be prevented. There needs to be a strong enough verification process to show the extent to which commitments have been fulfilled. Audits should be regular, in a similar way to Sarbanes-Oxley external audit, rather than one-off checks at the accountability programme level. Note, however, that missing evidence can pose a problem, and guarantees are needed about the integrity and authenticity of evidence supporting this verification and the account. In addition, the actor carrying out the verification checks needs to be trusted by the data subject and needs to have the appropriate authority and resources to carry out spot checking and other ways of asking organisations to demonstrate accounts.

It is therefore important that the data protection officer is truly independent and does not collude with the organisation. Equally, that any external parties involved in holding the organisation to account do not collude with the organisation, for example by rubber stamping, revolving door opportunities, etc.

Q2.2.6. Please share your views on whether organisations are likely to maintain a similar data protection officer role, if not mandated?

JAAG believes that organisations may not maintain a similar data protection officer role, if not mandated because it will cost extra and be viewed as a "grudge spend". This effectively removes much of the accountability element, and could be disastrous in extreme cases.

Q2.2.7. To what extent do you agree with the following statement: 'Under the current legislation, data protection impact assessment requirements are helpful in the identification and minimisation of data protection risks to a project'?
○ Strongly agree

Q2.2.7a. Please explain your answer, and provide supporting evidence where possible.

DPIAs are designed to identify and help minimise data protection risks in a project, and are an effective way of doing so. They are also targeted mainly at the higher risk activities which really do need this kind of scrutiny.

Q2.2.8. To what extent do you agree with the proposal to remove the requirement for organisations to undertake data protection impact assessments?
○ Strongly disagree

Q2.2.8a. Please explain your answer, and provide supporting evidence where possible, and in particular describe what alternative risk assessment tools would achieve the intended outcome of minimising data protection risks.

JAAG firmly rejects the proposal to remove the requirement for organisations to undertake data protection impact assessments. It is a deeply worrying proposal which could well result in a high level of harm to individual citizens and to society.

Prior consultation requirements

Q2.2.9. Please share your views on why few organisations approach the ICO for 'prior consultation' under Article 36 (1)-(3). As a reminder Article 36 (1)-(3) requires that, where an organisation has identified a high risk that cannot be mitigated, it must consult the ICO before starting the processing. Please explain your answer, and provide supporting evidence where possible.

Not all organisations, or groups within organisations, are aware of their data protection responsibilities. Others may be aware but hope that ICO will not have enough resources to detect their illegal activities. Others hope to stay 'under the radar' but consider it a business risk worth running given that any fines will be unlikely or low enough to justify ignoring their responsibilities. Of course, this also applies to accountability-based frameworks: some organisations will take the same approach. A big deterrent to this type of behaviour would be if the ICO were to be able to levy very significant fines and have enough resources and independence to investigate such organisations proactively and vigorously.

Q2.2.10. 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'?
○ Somewhat agree

Q2.2.10a. 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?

This may well be the case, but this does not make it the right thing to do! However, if the organisations show that they have been investing in doing the right thing and appropriate governance procedures and trying hard, this would realistically be taken into account, to some extent, in many cases. Further incentives would be high penalties for doing the wrong thing (and the ICO would help show how to avoid that) and high probability of being found out. The example of the UK water companies is something we need to avoid. Here, fines appear to be cheaper than investment in mitigating pollution, etc., with the result that our coastal waters and rivers are awash with millions of gallons of untreated sewage. A useful example of an incentivised scheme is the Environment Agency's Operator Monitor Assessment (OMA) scheme. Environmental inspections

become less frequent, and therefore less costly when the plant operator uses appropriately certified devices and software. This incentivises investment in suitable techniques and measures.

Q2.2.11. To what extent do you agree with the proposal to reduce the burden on organisations by removing the record keeping requirements under Article 30?
○ Strongly disagree

Q2.2.11a. Please explain your answer, and provide supporting evidence where possible.

Providing accounts is a central part of an accountability-based approach! Moreover, these accounts should be understandable to the target audience, and should be accurate. Furthermore, not only accounts must be available, but also the logged data on which they are based should be stored for a suitable period so that, for example, accounts can be revised in the event of the later discovery of software bugs which might affect the integrity of a published version of the accounts. The particular documentation requirements should be proportionate to the size of the organisations, by taking small and medium size enterprises into account. However, if a small organisation engages in high-risk data processing, the accountability requirements must be more rigorous.

Q2.2.12. 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?
○ Strongly disagree

Q2.2.12a. Please explain your answer, and provide supporting evidence where possible and in particular
JAAG strongly disagrees with the proposal to reduce burdens on organisations by adjusting the threshold for notifying personal data breaches to the ICO under Article 33. Citizens cannot make informed choices unless they are given important information affecting that choice. Organisations cannot be held accountable if relevant information is not provided to the entities holding that organisation to account. There are laws that penalise citizens for failing to report accidents. A personal data breach can be an accident, but it should still always be reported. For example, the misuse of "BCC" might, in a way unknown to the perpetrator, lead to the disclosure of an email address belonging to the victim of domestic abuse.

Q2.2.12a1. Would the adjustment provide a clear structure on when to report a breach?

JAAG is not clear that the adjustment would provide a clear structure on when to report a breach; it would seem that it would have to be a substantial and serious type of breach, but how a data breach affecting an individual might fit that category is not clear, as privacy harm is notoriously difficult to quantify. Many harms, and aggregated harms, or breaches of individual rights, are likely to be ignored. ICO may be able to define a clear structure, but whether it will be a good approach for citizens is another matter. Given the other proposals, there is a real possibility that ICO would not have the resources to police this adequately. JAAG is concerned that the ICO will be subjected to successive reductions in resources so that its ability to operate effectively will be reduced. This has already happened with Trading Standards, see the Unison report *Trading standards – how cuts are putting individuals and communities at risk and damaging local businesses and economies.*

Q2.2.12a2. Would the adjustment reduce burdens on organisations?

Yes, it probably would reduce burdens, but it is also likely to encourage under-reporting or less investment in breach notification checks and procedures. It is also likely to lead to an increase in harm to individuals.

Q2.2.12a3. What impact would adjusting the threshold for breach reporting under Article 33 have on the rights and freedoms of data subjects?

Adjusting the threshold for breach reporting under Article 33 would go against the transparency principle, and could affect the security principle as appropriate changes may not be made, and could also affect data subjects' choice and control. It may also encourage organisations not to concern themselves with aggregated breaches of personal data and not to invest in preventing these, but rather to focus only on whatever is required in terms of reporting.

Q2.2.13. To what extent do you agree with the proposal to introduce a voluntary undertakings process? As a reminder, in the event of an infringement, the proposed voluntary undertakings process would allow accountable organisations to provide the ICO with a remedial action plan and, provided that the plan meets certain criteria, the ICO could authorise the plan without taking any further action.

○ Strongly disagree

Q2.2.13a. Please explain your answer, and provide supporting evidence where possible.

JAAG strongly disagrees with the proposal to introduce a voluntary undertakings process. The strong penalties allowable under GDPR do oblige companies to invest in better practices. If self-regulation is allowed and if, as proposed in paragraph 157, an organisation whose privacy management programme does not meet the required standards is asked by the ICO to make improvements to its privacy management programme, this would not be sufficient deterrent against ignoring legal requirements.

Q2.2.14. Please share your views on whether any other areas of the existing regime should be amended or repealed in order to support organisations implementing privacy management requirements.

Any amendments should be in line with encouraging strong accountability,

Q2.2.15. What, if any, safeguards should be put in place to mitigate any possible risks to data protection standards as a result of implementing a more flexible and risk-based approach to accountability through a privacy management programme?

It appears that flexible and risk-based approaches are being taken as central aspects of a privacy management programme. This does not mean that individuals' data rights must be, or indeed, should be, swept away as part of a privacy management programme. Yet it appears that the proposals have this in mind. JAAG finds this to be a very worrying development from a citizens' point of view because the only remaining lines of defence left to citizens would be (a) to trust organisations, whose primary motive is often an economic one, at odds with their individual and collective interests including self-determination and privacy, and (b) the data protection regulator (ICO), but there is a real risk that the other proposals would severely limit the effectiveness of the ICO in standing up for citizens' rights.

A better way forward is to take a strong accountability approach, with all the safeguards involved, including properly resourcing the ICO, rather than eroding individuals' privacy rights.
In essence, to meet the various ethical, social and legal obligations that apply to their business situation, organizations should:

- Embed accountability into their culture and practices
- Integrate ethical decision making into their operations… i.e. embed it into the operations and not just engage a separate organization to do that
- Employ privacy by design, but also widen that to include other ethical dimensions such as fairness
- Use good security

2.2 Alt approach. The questions below relate to alternative reform proposals should privacy management programmes not be introduced.

Q2.2.16. To what extent do you agree that some elements of Article 30 are duplicative (for example, with Articles 13 and 14) or are disproportionately burdensome for organisations without clear benefits?

Q2.2.16a. Please explain your answer, and provide supporting evidence where possible, and in particular address which elements of Article 30 could be amended or repealed because they are duplicative and/or disproportionately burdensome for organisations without clear benefits.

Q2.2.17. To what extent do you agree that the proposal to amend the breach reporting requirement could be implemented without the implementation of the privacy management programme?
○ Somewhat disagree

Q2.2.17a. Please explain your answer, and provide supporting evidence where possible

Implementation of a privacy management programme would be a good thing to ensure that organisations consider privacy properly throughout their operations, but of course it need not take the form of the risk-based approach cited. The breach reporting requirement might be relaxed, but if organisations do not improve their privacy procedures so that they ~~are~~ check~~ing~~ that they are at least in compliance with legal requirements, and ideally setting a higher ethical bar, then the overall situation would be worsened rather than made better.

Q2.2.18. To what extent do you agree with the proposal to remove the requirement for all public authorities to appoint a data protection officer?
○ Somewhat disagree

Q2.2.18a. Please explain your answer, and provide supporting evidence where possible.

It seems questionable that requirements for public bodies are not the same as for private bodies, but the additional overhead for small public bodies seems justified when balanced against the risks of removing the requirement entirely.

Q2.2.19. If you agree, please provide your view which of the two options presented at paragraph 184d(V) would best tackle the problem.
Q2.2.19.a. Please provide supporting evidence where possible, and in particular:

What risks and benefits you envisage
Q2.2.19.b. What should be the criteria for determining which authorities should be required to appoint a data protection officer

Q2.2.20. If the privacy management programme requirement is not introduced, what other aspects of the current legislation would benefit from amendments, alongside the proposed reforms to record keeping, breach reporting requirements and data protection officers?

JAAG considers these amendments not beneficial. The focus should be on introducing a privacy management programme together with strong accountability provisions.

2.3. Subject Access Requests

Q2.3.1. Please share your views on the extent to which organisations find subject access requests time-consuming or costly to process.

Q2.3.1a. Please provide supporting evidence where possible, including:

Q2.3.1a1. What characteristics of the subject access requests might generate or elevate costs

If an automated system has been put in place to deal with such requests, then the unit cost of addressing a request would normally be very low. Some organisations do not make such an investment because they have a very low rate of requests and just handle those by hand. Should the numbers suddenly increase, then they can easily become overwhelmed. Those organisations should really be investing in more efficient procedures in order to meet legal requirements - that is an appropriate solution rather than deciding to restrict subject access requests as being inconvenient.

It should be noted that where legislation imposes requirements for reporting, software suppliers see a gap in the market and come up with products to meet that demand. For example, requirements for safeguarding children and vulnerable adults has led to the development of several useful logging, tracking, and reporting software products. The deployment of these leads, in our experience, to greater levels of trust among parents, etc.

Q2.3.1a2. Whether vexatious subject access requests and/or repeat subject access requests from the same requester play a role
Q2.3.1a3. Whether it is clear what kind of information does and does not fall within scope when responding to a subject access request

Q2.3.2. To what extent do you agree with the following statement: 'The 'manifestly unfounded' threshold to refuse a subject access request is too high'?
○ Strongly disagree

Q2.3.2a. Please explain your answer, providing supporting evidence where possible, including on what, if any, measures would make it easier to assess an appropriate threshold.

Q2.3.3. To what extent do you agree that introducing a cost limit and amending the threshold for response, akin to the Freedom of Information regime (detailed in the section on subject access requests), would help to alleviate potential costs (time and resource) in responding to these requests?
○ Strongly disagree

Q2.3.3a. Please explain your answer, and provide supporting evidence where possible, including on:
Q2.3.3a1. Which safeguards should apply (such as mirroring Section 16 of the Freedom of Information Act (for public bodies) to help data subjects by providing advice and assistance to avoid discrimination?
Q2.3.3a2. What a reasonable cost limit would look like, and whether a different (i.e. sliding scale) threshold depending on the size (based on number of employees and/or turnover, for example) would be advantageous

Introducing a cost limit and amending the threshold for response, might well help to alleviate potential costs in responding to these requests, however, this cannot be an overriding factor if the result is to make it more difficult for citizens to exercise their rights. If a body might hold sensitive information about a citizen, for example, it is reasonable for that citizen to wish to know what information it holds and what it might do with it; and moreover, to be able to object to that, without having additional barriers put in the way. The vulnerable in our society would be especially affected.

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 disagree

Q2.3.4a. 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.

The introduction of even a low fee would set an undermining precedent which might leave the way open for fees to be raised to a level that deters people from exercising their rights. There is no need to change the existing arrangement.

Q2.3.5. Are there any alternative options you would consider to reduce the costs and time taken to respond to subject access requests?

Q2.3.5a. Please explain your answer, and provide supporting evidence where possible.

2.4. Privacy and electronic communications

Q2.4.1. What types of data collection or other processing activities by cookies and other similar technologies should fall under the definition of 'analytics'?

Purely anonymous information used for statistical analysis across large numbers of users. The acquired data should not be capable of being de-anonymised or otherwise used to identify individual data sources and individuals.

Q2.4.2. To what extent do you agree with the proposal to remove the consent requirement for analytics cookies and other similar technologies covered by Regulation 6 of PECR?
○ Somewhat disagree

Q2.4.2a. Please explain your choice, and provide supporting evidence where possible, including what safeguards should apply.

It is better that users have choice, control and transparency about what information is being collected, and why. Also, if the proposal went ahead, there is a worry that some mechanisms could be added to this category that the user might be very uncomfortable with.

Q2.4.3. To what extent do you agree with what the Government is considering in relation to removing consent requirements in a wider range of circumstances? Such circumstances might include, for example, those in which the controller can demonstrate a legitimate interest for processing the data, such as for the purposes of detecting technical faults or enabling use of video or other enhanced functionality on websites.
○ Strongly disagree

Q2.4.3a. Please explain your answer, and provide supporting evidence where possible, including what circumstances should be in scope and what, if any, further safeguards should apply.

Informational self-determination is an important right and should not be eroded.

Q2.4.4. To what extent do you agree that the requirement for prior consent should be removed for all types of cookies?
○ Strongly disagree

Q2.4.4a. Please explain your answer, and provide supporting evidence where possible. Please explain how organisations could comply with the UK GDPR principles on lawfulness, fairness and transparency if PECR requirements for consent to all cookies were removed.

Q2.4.5. Could sectoral codes (see Article 40 of the UK GDPR) or regulatory guidance be helpful in setting out the circumstances in which information can be accessed on, or saved to a user's terminal equipment?

Perhaps, but much will depend upon who will check whether this is being done, and what the penalties would be for non compliance.

Q2.4.6. What are the benefits and risks of requiring websites or services to respect preferences with respect to consent set by individuals through their browser, software applications, or device settings?

The benefit is that individuals have some control at least over the increasingly pervasive surveillance that is being carried out on them. The risks are that the service providers do not comply with the requirements, or deliberately mislead individuals to get them (e.g. via clicking buttons with ambiguous text) to allow broader consent settings than the individuals intended.

Q2.4.7. How could technological solutions, such as browser technology, help to reduce the volume of cookie banners in the future?

Q2.4.8. What, if any, other measures would help solve the issues outlined in this section?

Opt-in definition. Under PECR, Businesses can generally only contact individuals who have previously been in touch during a sale or transaction, and have not refused or opted out of receiving marketing communications about similar products. This is known as a 'soft opt-in'.

Q2.4.9. To what extent do you agree that the soft opt-in should be extended to non-commercial organisations?

Q2.4.9a. Please explain your answer, and provide supporting evidence where possible.

Q2.4.10. What are the benefits and risks of updating the ICO's enforcement powers so that they can take action against organisations for the number of unsolicited direct marketing calls 'sent'? Currently the ICO can only take action on calls which are 'received' and connected. The ICO sometimes receives intelligence of companies sending thousands of calls but which are not all connected, but they cannot take account of the potential risk of harm when determining the most appropriate form of enforcement action.

The benefit is to deter this type of annoying behaviour. We do not see a risk.

Q2.4.11. What are the benefits and risks of introducing a 'duty to report' on communication service providers?
This duty would require communication service providers to inform the ICO when they have identified suspicious traffic transiting their networks. Currently the ICO has to rely on receiving complaints from users before they can request relevant information from communication service providers.
Please provide information on potential cost implications for the telecoms sector of any new reporting requirements.

The benefit is that this information could be useful to ICO in performing their role. The risk is that ICO could be inundated with information that it does not really need, and that is costly for the service providers to gather and send. Guidance should come from ICO on what type of information they wish to receive from providers.

Q2.4.12. What, if any, other measures would help to reduce the number of unsolicited direct marketing calls and text messages and fraudulent calls and text messages?

Q2.4.13. Do you see a case for legislative measures to combat nuisance calls?
○ Yes

Q2.4.13a. If yes, what measures do you propose and why?
If no, please explain your answer, and provide supporting evidence where possible.

Q2.4.14. What are the benefits and risks of mandating communications providers to do more to block calls and texts at source?

Q2.4.15. What are the benefits and risks of providing free of charge services that block, where technically feasible, incoming calls from numbers not on an 'allow list'? An "allow list" is a list of approved numbers that a phone will only accept incoming calls from.

Q2.4.16. To what extent do you agree with increasing fines that can be imposed under PECR so they are the same level as fines imposed under the UK GDPR (i.e. increasing the monetary penalty maximum from £500,000 to up to £17.5 million or 4% global turnover, whichever is higher)?
○ Somewhat agree

Q2.4.16a. Please explain your choice, and provide supporting evidence where possible.

Stronger penalties generally encourage compliance and discourage fraudsters.

Q2.4.17. To what extent do you agree with allowing the ICO to impose assessment notices on organisations suspected of infringements of PECR to allow ICO to carry out audits of the data controllers' processing activities?
○ Strongly agree

Q2.4.17a. Please explain your choice, and provide supporting evidence where possible.

JAAG considers this to be a good idea. It is our experience that audits are an effective way of discovering software defects, infringements, and other shortcomings. The ICO should be empowered and resourced adequately to ensure that audits can be undertaken promptly and effectively.

Q2.4.18. Are there any other measures that would help to ensure that PECR's enforcement regime is effective, proportionate and dissuasive?

Q2.4.18a. If yes, what measures do you propose and why?

2.5. Use of personal data for the purposes of democratic engagement

Q2.5.1. To what extent do you think that communications sent for political campaigning purposes by registered parties should be covered by PECR's rules on direct marketing, given the importance of democratic engagement to a healthy democracy?

We do not think that there should be any change from the current position. We agree that political parties should not call, email or text prospective voters for purposes such as campaigning or fundraising, unless they have obtained prior consent.

Q2.5.1a. Please explain your answer, and provide supporting evidence where possible.

It could be very dangerous to relax the laws under the pretext of increasing democratic engagement. There are many harms that could arise, and in fact do arise in other countries where the laws are weaker on this point. Detailed profiles about individual voters and their political beliefs and other protected characteristics could be created without the voters' knowledge or consent. Furthermore, these could then be used to create customised political marketing material designed to appeal to specific voters and which excluded information judged to be disliked by them. This has the effect of reducing voters' ability to properly engage with political debate and make up their minds, because they are being provided less and less with independent material but rather with very biased material tailored to influence them to vote in a particular way. Expansion of the uses of data from the electoral register would indeed result in a decrease in trust, as mentioned in paragraph 225.

Q2.5.2.. If you think political campaigning purposes should be covered by direct marketing rules, to what extent do you agree with the proposal to extend the soft opt-in to communications from political parties?
○ Neither agree nor disagree

Q2.5.2a. Please explain your answer, and provide supporting evidence where possible.

Q2.5.3. To what extent do you agree that the soft opt-in should be extended to other political entities, such as candidates and third-party campaign groups registered with the Electoral Commission?
○ Somewhat agree

Q2.5.3a. Please explain your answer, and provide supporting evidence where possible.

A level playing field is the fairest approach.

Q2.5.4.. To what extent do you think the lawful grounds under Article 6 of the UK GDPR impede the use of personal data for the purposes of democratic engagement?
○ Strongly disagree

Q2.5.4a. Please explain your answer, and provide supporting evidence where possible.

It would be very worrying if we change our legislation to allow us to be more like the US in the sense of allowing analytics to be used on information gathered about citizens so that political parties form and update databases of individual voters' likely voting intentions and use these to target 'swing' voters only with differing information targeted at what they were likely to want to hear, etc. This actually runs very much in the face of democratic engagement, as all citizens are not presented with a common manifesto and encouraged to make up their minds about a party's promises and enter into debate, but rather surveilled, managed and manipulated on an individual level with half truths and only part of the story. It is informational gerrymandering: with politicians and their parties choosing the voters, rather than the voters electing the politicians.

Q2.5.5. To what extent do you think the provisions in paragraphs 22 and 23 of Schedule 1 to the DPA 2018 impede the use of sensitive data by political parties or elected representatives where necessary for the purposes of democratic engagement?
○ Strongly disagree

Q2.5.5a. Please explain your answer, and provide supporting evidence where possible.

Moving further in the direction of allowing political parties to process sensitive data about people's political opinions without consent would be very worrying. It is just not the case that this would in general help democratic engagement in any meaningful sense, but rather, it is likely to result in even more political profiling and sophisticated techniques of persuasion based upon that. Furthermore, risks of discrimination are opened up, especially if more authoritarian regimes gain power.

2.6. Further Questions

Q2.6.1. In your view, which, if any, of the proposals in 'Reducing Burdens on Businesses and Delivering Better Outcomes for People', would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

Payment for subject access requests.

Q2.6.2. In addition to any of the reforms already proposed in 'Reducing burdens on business and delivering better outcomes for people', (or elsewhere in the consultation), what reforms do you think would be helpful to reduce burdens on businesses and deliver better outcomes for people?

There are service providers (SPs) who offer database management, customer relationship management, and other functions to both companies and charities. The latter are often granted free access up to a certain number of "seats". The SP handles all matters relating to GDPR, etc. If there was a cohort of trusted SPs, certified by an accredited certifying body, then this would be helpful, especially to smaller enterprises. If the standards they worked to were ethical ones then this would also help eliminate the 'cowboys', as has proved the case in other markets.

Q2.6.3. In addition, the Government would welcome views on the desirability of consolidating the UK GDPR and the Data Protection Act 2018.

GDPR and Data Protection Act complement each other, but GDPR supersedes the latter. If there were a consolidation, the GDPR should take precedence. JAAG is concerned that in the 'consolidation' process the GDPR will be watered down.

Q2.6.3a. End of chapter Q. Do you have any general comments about this chapter not yet captured by your responses to the questions above?

Chapter 3 Boosting trade and reducing barriers to data flows

3.2. Adequacy

Q3.2.1. To what extent do you agree that the UK's future approach to adequacy decisions should be risk-based and focused on outcomes?
○ Somewhat disagree

Q3.2.1a. Please explain your answer and provide supporting evidence if possible.

UK should take care not to enter into agreements whereby personal data may be transferred in the same way as within the UK, with other countries that do not have a legislative framework that protects such data to the same standard as the European one. This is why GDPR has a concept of adequacy. There are ways that business may be allowed, in certain contexts, to do this through standard model contracts, etc., by which means it can be shown that the environment into which the data passes is of a similar standard.

The proposal that, instead, decisions should be risk-based and focused on outcomes, could lead to cases where personal (including sensitive) information will be at risk in many different ways. One source of risk may be relatively weak self-certification by organisations who operate without a strong legal framework to back up any issues, including redress. This approach could be very damaging, depending on what exactly it involved. Another risk is that by adopting this approach, the UK will no longer be considered adequate by the EU, which will be very disruptive to business. In addition, if the UK Human Rights Act 1998 is weakened, this will further reduce the standard required for adequacy assessments.

Q3.2.2. To what extent do you agree that the government should consider making adequacy regulations for groups of countries, regions and multilateral frameworks?
○ Neither agree nor disagree

Q3.2.2a. Please explain your answer, and provide supporting evidence where possible.

If these adequacy regulations were not equivalent to European standards, then there is not only a risk to citizens' data but also a risk that the EU may consider that the UK is to be judged as being not adequate. Furthermore, a country's cultural context may have a local impact e.g. in some cases identification of employees is poor and staff turnover is high, encouraging the planting of employees specifically to steal high value sensitive information and then disappear.

Q3.2.3. To what extent do you agree with the proposal to strengthen ongoing monitoring of adequacy regulations and relax the requirement to review adequacy regulations every four years?
○ Neither agree nor disagree

Q3.2.3a. Please explain your answer, and provide supporting evidence where possible.

If the monitoring is as comprehensive as a review, then having it repeated more often than 4 years, and triggered by certain external changes, might be beneficial, although presumably it would involve additional resources. An annual surveillance audit - conducted remotely and via forms - would probably reduce the scope of four-yearly review. Experience in the environmental sector shows that both are useful.

Q3.2.4. To what extent do you agree that redress requirements for international data transfers may be satisfied by either administrative or judicial redress mechanisms, provided such mechanisms are effective?
○ Neither agree nor disagree

The government needs to provide more detail before consultees can make a judgement on this. For example, if redress includes compensating data subjects for harms, we would need to know on what basis this would be decided. Improved redress mechanisms would certainly be welcome.

Q3.2.4a. Please explain your choice, and provide supporting evidence where possible.

It would be better if judicial redress took place in the countries where the affected data subjects reside, in order to facilitate their involvement and to better reflect the rights that they expect. However, the government needs to clarify who would make the choice between these forms of redress, and who would judge whether administrative redress was unsatisfactory or inadequate.

3.3. Alternative Transfer Mechanisms

Q3.3.1. To what extent do you agree with the proposal to reinforce the importance of proportionality when assessing risks for alternative transfer mechanisms?
○ Somewhat disagree

Q3.3.1a. Please explain your answer, and provide supporting evidence where possible.

JAAG is concerned that there is a risk that individual rights could be diminished, and the interests of the vulnerable in society could be sidelined, by the profit motive. If a putative value is allocated to these rights and interests and is then compared with the value of other financial interests, the way in which these are modelled and valued becomes of crucial importance, likewise the way in which the comparison will be assessed and checked. JAAG believes it is likely that these individual valuations will be at a level that will not be able to compete with those of big business interests. The focus needs to be on avoiding potential harms to individuals and society, not the profit motive. Previous legal frameworks have taken a principles-based approach that incorporates human rights. Here, certain actions are mandated or prohibited, or at least required to be weighed and justified if they are to be trumped by other considerations. Without legal frameworks, there is little to protect individuals if organisations do not choose to take an ethical approach and regulators are not given enough resources to make thorough checks or enough clout to issue fines that encourage compliance.

Q3.3.2. 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?

Q3.3.3. 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?
○ Somewhat disagree

Q3.3.3a. Please explain your answer, and provide supporting evidence where possible.

The universality of human rights fits ill with this decision. The personal data originating overseas might have been sent there from other countries, and might even correspond to UK or EU citizens; if so, this approach would not work. There would need to be a system to check this.

Q3.3.4. 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?
○ Somewhat disagree

Q3.3.4a. Please explain your answer, and provide supporting evidence where possible.

These mechanisms would need to be checked by the regulator or a suitably accredited independent party, who would have to be adequately resourced. The process would need to mitigate against the risks that the mechanisms would rely on self-certification or not attain the expected standard.

Q3.3.5. 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?

Q3.3.6. 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?
○ No

It is proposed that the ICO assess individual countries' adequacy on a regular basis, so this less trustworthy assessment is inappropriate. The interval between adequacy assessments must be sufficiently short to prevent low standards being followed. This implies that the ICO must have suitable resources for this work.

Q3.3.6a. Please explain your answer, and provide supporting evidence where possible.
It is unclear by whom the assessment would be made.

Q3.3.7. 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?
○ Strongly disagree

It would certainly be flexible, yet unsafe, cheap to run, costly to harmed individuals, and unaccountable.

Q3.3.7a. Please explain your answer, and provide supporting evidence where possible.

Q3.3.8. Are there any mechanisms that could be supported that would benefit UK organisations if they were recognised by the Secretary of State?

Q3.3.8a. Please explain your answer, and provide supporting evidence where possible.

3.4. UK certification schemes

Q3.4.1. 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?

Q3.4.1a. Please explain your answer, and provide supporting evidence where possible.

Q3.4.2. To what extent do you agree that allowing accreditation for non-UK bodies will provide advantages to UK-based organisations?
Q3.4.2a. Please explain your answer, and provide supporting evidence where possible.

Q3.4.3. Do you see allowing accreditation for non-UK bodies as being potentially beneficial for you or your organisation?
Q3.4.3a. Please explain the advantages and risks that you foresee for allowing accreditation of non-UK bodies.

Q3.4.4. Are there any other changes to certifications that would improve them as an international transfer tool?

3.5. Derogations

Q3.5.1. 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?
Q3.5.1a. Please explain your answer, and provide supporting evidence where possible.

3.6. Further questions

Q3.6.1. The proposals in this chapter build on the responses to the National Data Strategy consultation. The Government is considering all reform options in the round and will carefully evaluate responses to this consultation. The Government would welcome any additional general comments from respondents about changes the UK could make to improve its international data transfer regime for data subjects and organisations.

Q3.6.2. In your view, which, if any, of the proposals in 'Boosting Trade and Reducing Barriers to Data Flows' would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

Q3.6.3. In addition to any of the reforms already proposed in 'Boosting Trade and Reducing Barriers to Data Flows' (or elsewhere in the consultation), what reforms do you think would be helpful to make the UK's international transfer regime more user-friendly, effective or safer?

Q3.6.3a. End of chapter Q. Do you have any general comments about this chapter not yet captured by your responses to the questions above?

Chapter 4 Delivering better public services

4.2. Digital Economy Act 2017

Q4.2.1. To what extent do you agree with the following statement: 'Public service delivery powers under section 35 of the Digital Economy Act 2017 should be extended to help improve outcomes for businesses as well as for individuals and households'?
Q4.2.1a. Please explain your answer, and provide supporting evidence where possible.

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'?
Q4.3.1a. Please explain your answer, and provide supporting evidence where possible.

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

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

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

4.4. Building Trust and Transparency

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

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

This seems an excellent idea. Public transparency about what algorithms do can make a difference. Here is a positive example, where the city of Amsterdam has started a register of artificial intelligence systems and algorithms used by the city authorities that can be inspected by the public (https://algoritmeregister.amsterdam.nl/en/holiday-rental-housing-fraud-risk/). This demonstrates their ethical and social justice credentials. Transparency is one of the principles that an AI system should have in order to be trustworthy, defined recently by the EU High-Level Expert Group on Artificial Intelligence, which has produced an ethics framework for AI.

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

As mentioned in paragraph 290, it would be helpful to have more detailed information about how ethical considerations are addressed. It would also be useful to integrate transparency about other elements of the ethics framework mentioned above, including privacy and sustainability.

For dataset consumers, standardised transparency along the lines of that described in the following paper would be very useful: Datasheets for Datasets (arxiv.org).
(https://arxiv.org/pdf/1803.09010.pdf)

The nature of accounts should be public where possible, and there is also a need for the commitments of the Data Controller (DC) (in this case the public body) to be properly understood by citizens (and other parties). In addition, the mechanisms used and relevant properties of the service providers in the provision chain need to be clarified as appropriate to customers and regulators. Furthermore, DPIA/PIA is one form of verification for accountability which should be used in conjunction with others. It can be used to help provide transparency about the nature of the risks, including the criteria used in the risk assessment; how decisions are made to mitigate risk, and whether the mechanisms to be used and implemented are appropriate for the context. Transparency would be further increased by comprehensive obligations for controllers to inform supervisory authorities and data subjects of personal data breaches. It is not only customers and end users that might be affected by certain kinds of data processing, but society at large. Transparency should therefore also be aimed at the general public and the regulator. This contributes to the maintenance of ethical standards, rather than stimulating a race to the bottom (of cost and privacy protection).

Trustworthy evidence should also be provided, for example using automated evidence gathering about non-compliance. Accountability evidence needs to be provided at a number of layers. At the organisational policies level, this would involve provision of evidence that the policies are appropriate for the context, which is typically what is done when privacy seals are issued. But this alone is rather weak. In addition, evidence can be provided about the measures, mechanisms and controls that are deployed and how they are configured, to show that these are appropriate for the context. For higher risk situations, continuous monitoring may be needed to provide evidence that what is claimed in the policies is actually being met in practice. Even if this is not sophisticated, some form of checking the operational running and feeding this back into an organisation's accountability management program in order to improve it, is part of accountability practice.

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

Transparency should be increased, in ways that do not decrease privacy or security. Where this would happen, the transparency should be tailored, e.g. via use of privacy enhancing technologies or by releasing meta-information only or by releasing information to trusted parties, or a combination of these.

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

Q4.4.4a. Please explain your answer and provide supporting evidence where possible, including on:
Q4.4.4a1. What, if any, situations are not adequately covered by existing provisions?
Q4.4.4a2. What, if any, further safeguards or limitations may be needed for any new situations?

The inclusion of new situations on the list should be specifically agreed by civil society, including citizens' representative groups, at the very least.

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

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

Yes, but it may nevertheless be a helpful distinction. It may also of course be difficult to determine whether processing is indeed in the public interest, especially if some groups would benefit and others would not.

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

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

Q4.4.6a1. What the risks and benefits of a definition would be
It may be difficult to predict what future benefits would really be, as well as appreciate future harm. If decisions are made in the public interest, it needs to be clear and non-controversial that this is the case, and this definition should when made fit this category i.e. be clearly in the public interest, and accepted as such by citizens and citizens' representative groups. It could, for example, be reviewed at intervals so that matters of current concern can be considered against the definition.

Q4.4.6a2. What such a definition might look like

JAAG believes that relevant factors to consider include how much benefit and harm is implied for different numbers and groups of people. However, the default position - that sensitive data cannot be processed unless there is explicit consent from the data subject, or it is expressly permitted for purposes listed in the existing UK GDPR and Schedule 1 to the DPA 2018 - seems very reasonable to us. We see no reason to alter it. Any modification might lead citizens to be concerned about how their data might be collected, shared and (ab)used as a result.

Q4.4.6a3. What, if any, safeguards may be needed?

JAAG believes that the interests of minority groups, and especially the vulnerable, need to be protected even if the majority might benefit. Individuals have rights, and certain rights should not be waived just because several others might benefit from them. This has to do with the sort of society that we want to live in, and the values that we in the UK have inherited from the past and hold dear e.g. from the Enlightenment and human rights promises after the atrocities of WW2.

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

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

JAAG believes that as commented above, this seems a risky action and would need to be done with the express support of civil society representatives.

Q4.4.7a1. What such situations may be

We cannot think of any new situations that would merit such an approach.

Q4.4.7a2. What the risks and benefits of listing those situations would be
Q4.4.7a3. What, if any, safeguards may be needed?

Quite apart from the proposed increase in processing of citizens' sensitive data, which poses increased risks, there is a particular danger that broad categories could be added that allow many different types of activity (e.g. 'safeguarding national security' could be used very broadly), or that insufficient oversight or justification is provided about usage.

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

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

JAAG believes that it is inappropriate to focus on transparency and public safety without also considering privacy. 'Streamlining' must not have the effect of making it easier for public (and commercial) bodies to deploy facial recognition and other biometric systems, because of the many risks and known problems this involves. We note, for example, the recent lack of transparency to citizens concerning a UK council's trial of facial recognition software. See for example https://walthamforestecho.co.uk/councils-facial-recognition-trial-should-concern-us-all/
JAAG believes that the government's focus should be on the known solutions and frameworks for using biometrics in a privacy-friendly way. It should not remove existing protections for citizens. See for example: Dilemmas of Privacy cover (raeng.org.uk) (https://www.raeng.org.uk/publications/reports/dilemmas-of-privacy-and-surveillance-report)

4.5. Public Safety and National Security

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

JAAG believes that this would undermine GDPR definitions and therefore weaken the legislation; terminology and definitions need to be accompanied by relevant standards.

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

4.6. Further Questions

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

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

Q4.6.2a. End of chapter Q. Do you have any general comments about this chapter not yet captured by your responses to the questions above?

It is good that the issue of trust is raised, because in order to capitalise on the potential benefits of emerging technologies, citizens should trust that these are deployed in an ethical and appropriate manner, for the public good. This applies not just to public services but also to privately provided services and goods. Prior research has been carried out on the nature of trust and how trusted technologies might be developed. In addition, ethical frameworks have been produced over a range of domains, and guidance has been provided on how to produce trustworthy AI (notably by IEEE and by ethics experts commissioned by EU). However, in the data protection area, there are unfortunately many examples where corporate interests have been put above the public good, to the detriment of society: see for example Shoshana Zuboff, “The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power”. This provides strong evidence that there are groups of people with a great deal of power and their own agendas who are not safeguarding the natural rights of people. This is a very grave matter. Care should be taken by the government that the proposals in this consultation do not make this situation worse. The governments’ proposals need to be modified considerably to avoid this, whilst still allowing innovation beneficial for society to go ahead, as that is also important and to be welcomed.

Chapter 5 Reform of the Information Commissioner's Office

5.2. Strategy, Objectives and Duties

Q5.2.1. To what extent do you agree that the ICO would benefit from a new statutory framework for its objectives and duties?
○ Strongly disagree

Q5.2.1a. Please explain your answer, and provide supporting evidence where possible.

The proposal to introduce a power for the Secretary of State for DCMS to prepare a statement of strategic priorities goes completely against the needed independence of ICO. Instead, what is really needed is greater resourcing of ICO so that it is able to do its job properly. This proposal looks like an attempt to hobble the ICO.

Q5.2.2. 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?
○ Strongly disagree

Q5.2.2a. Please explain your answer, and provide supporting evidence where possible.

There is no need for it, since the ICO has already defined strategies. There is nothing wrong with these proposed objectives per se, but it is unclear what is meant by them and why they should supersede what has already been declared in the Information Rights Strategic Plan. For example, it is proposed that data rights are upheld, but the government is proposing here to change the legislation and severely reduce GDPR data rights protections.

Q5.2.3. Are there any alternative elements that you propose are included in the ICO's overarching objective?
○ No

JAAG does not support a change from the ICO's current objectives.

Q5.2.3a. Please explain your answer, and provide supporting evidence where possible.

We wish to keep it as it is.

Q5.2.4. 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

Q5.2.4a. Please explain your answer, and provide supporting evidence where possible.

The ICO already does this, so there is no need for a new duty. Within the wording of what is proposed, it seems that this is very likely to result in a further increase in the imbalance of power, increasingly marginalising the interests and representation of civil society. Instead, the ICO, as "The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals", should focus on those aspects;

sometimes this focus on the public good will reflect economic growth and innovation but that cannot be paramount. Moreover, effective regulation leads to innovation, as in the successful environmental instrumentation market.

Q5.2.5. 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

Q5.2.5a. Please explain your answer, and provide supporting evidence where possible.

This is entirely inappropriate: it could lead to corporate profit to the detriment of the common good - increased harm to individuals, loss of privacy protections, etc.

Q5.2.6. To what extent do you agree with the proposal to introduce a new duty for the ICO to cooperate and consult with other regulators, particularly those in the Digital Regulation Cooperation Forum (CMA, Ofcom and FCA)?
○ Somewhat disagree

Q5.2.6a. Please explain your answer, and provide supporting evidence where possible.

JAAG does not believe it should be a duty. It is a good thing to make sure that aspects do not fall between the gaps, and indeed some co-operation and mutual consultation (as already exists) is a good thing. However, this should not stay the hand of the ICO if the other regulators favour different priorities, which seems to be what is being proposed. It runs the risk of slowing and compromising decision-making within the ICO.

Q5.2.7. Are there any additional or alternative regulators to those in the Digital Regulation Cooperation Forum (CMA, Ofcom and FCA) that the duty on the ICO to cooperate and consult should apply to?
○ No

Q5.2.7a. Please explain your answer, and provide supporting evidence where possible.

We do not think this duty should apply, still less to regulators less relevant to data protection.

Q5.2.8. To what extent do you agree with the establishment of a new information sharing gateway between relevant digital regulators, particularly those in the DRCF?
○ Neither agree nor disagree

Q5.2.8a. Please explain your answer, and provide supporting evidence where possible.

This rather depends upon the details and how it would be used. It may indeed be a good idea to share ideas and make sure that issues do not fall between the gaps.

Q5.2.9. Are there any additional or alternative regulators to those in the DRCF (ICO, CMA, Ofcom and FCA) that the information sharing gateway should include?
○ Don't know

Q5.2.9a. Please explain your answer, and provide supporting evidence where possible.

Q5.2.10. To what extent do you agree with the Government's proposal to introduce specific language recognising the need for the ICO to have due regard to public safety when discharging its functions?
○ Strongly disagree

Q5.2.10a. Please explain your answer and provide supporting evidence where possible.

No, the focus of the ICO should rather be on the public good. The ICO already decides what is in the public good and makes a balance between public safety and collective rights, which is exactly what is needed. This proposal risks tipping the balance more in the direction of public safety and thereby runs the risk of a less effective counterbalance to authoritarian activities and private surveillance of the public space.

Q5.2.11. To what extent do you agree with the proposal for the Secretary of State for DCMS to periodically prepare a statement of strategic priorities which the ICO must have regard to when discharging its functions?
○ Strongly disagree

Q5.2.11a. Please explain your answer, and provide supporting evidence where possible.

We strongly disagree. This would allow political control on an ongoing basis, affected very much by the government of the day. It would definitely not be in the public interest.

Q5.2.12. To what extent do you agree with the proposal to require the ICO to deliver a more transparent and structured international strategy?
○ Strongly disagree

Q5.2.12a. Please explain your answer, and provide supporting evidence where possible.

We strongly disagree with the proposal: it is unnecessary and could make ICO less independent.

Q5.2.13. To what extent do you agree with the proposal to include a new statutory objective for the ICO to consider the Government's wider international priorities when conducting its international activities?
○ Strongly disagree

Q5.2.13a. Please explain your answer, and provide supporting evidence where possible.

We strongly disagree with the proposal: it seems likely to result in more control for big business and the government of the day. It would be better to keep ICO independent and well resourced so that it can do its job, overseen by parliament.

5.3. Governance Model and Leadership

Q5.3.1. To what extent do you agree that the ICO would benefit from a new governance and leadership model, as set out above?
○ Somewhat disagree

Q5.3.1a. Please explain your answer, and provide supporting evidence where possible.

In recent years ICO has been a trustworthy representative of citizens. The most pressing change needed is to resource it properly so that it can have the opportunity to adequately check whether organisations are obeying the law. There is a danger with the proposed changes that the board membership would be indirectly controlled or influenced in its makeup by the government. In making these changes, the ICO's impartiality in regulating government and the public sector must be maintained.

Q5.3.2. To what extent do you agree with the use of the Public Appointment process for the new chair of the ICO?
○ Somewhat disagree

Q5.3.2a. Please explain your answer, and provide supporting evidence where possible.

We note that the ICO argues convincingly for the continuation of the Crown appointment for this role, and for clarity about the role government would have in relation to removal from post.

Q5.3.3. To what extent do you agree with the use of the Public Appointment process for the non-executive members of the ICO's board?
○ Neither agree nor disagree

Q5.3.3a. Please explain your answer, and provide supporting evidence where possible.

Clarity is needed on the role government would have in removal from post.

Q5.3.4. To what extent do you agree with the use of the Public Appointment process for the new CEO of the ICO?
○ Strongly disagree

Q5.3.4a. Please explain your answer, and provide supporting evidence where possible.

We strongly disagree with the proposal: The implication is that Ministers would be responsible for the final decision, and that the ICO would thereby be by constitution less independent from government than other regulators. The ICO believes that the Board should ultimately be responsible for this appointment and we agree.

Q5.3.5. To what extent do you agree that the salary for the Information Commissioner (i.e. the proposed chair of the ICO in the future governance model) should not require Parliamentary approval?
○ Somewhat disagree

Q5.3.5a. Please explain your answer, and provide supporting evidence where possible.

Transparency and accountability to parliament is generally beneficial.

5.4. Accountability and Transparency

Q5.4.1. To what extent do you agree with the proposal to strengthen accountability mechanisms and improve transparency to aid external scrutiny of the ICO's performance?
○ Somewhat disagree

Q5.4.1a. Please explain your answer, and provide supporting evidence where possible.

JAAG believes in the value of improving transparency about public bodies' organisational activities and strengthening accountability mechanisms. Such mechanisms and scrutiny must always be fully transparent and free from bias. To date, the ICO has succeeded in balancing citizens' interests and business interests in a way that benefits society and the economy.
We are not aware of any citizen pressure for change in this.
Furthermore, many elements of the proposed mandatory reporting are completely new objectives and priorities set by government, which add new political content and decrease the independence of the ICO.

Q5.4.2. To what extent do you agree with the proposal to introduce a requirement for the ICO to develop and publish comprehensive and meaningful key performance indicators (KPIs) to underpin its annual report?
○ Somewhat agree

Q5.4.2a. Please explain your answer, and provide supporting evidence where possible.

Agree, subject to ICO being in full control of setting the terms for this.

Q5.4.3. To what extent do you agree with the proposal to require the ICO to publish the key strategies and processes that guide its work?
○ Neither agree nor disagree

Q5.4.3a. Please explain your answer, and provide supporting evidence where possible.

It already does this. It isn't particularly a problem for it to be required to do so but it is a problem if the government wants to interfere in what these key strategies and processes are, thus making the ICO less independent and accountable to Parliament.

Q5.4.4. What, if any, further legislative or other measures with respect to reporting by the ICO would aid transparency and scrutiny of its performance?
○ No

Q5.4.4a. Please explain your answer, and provide supporting evidence where possible.
This question cannot be answered in a Yes/No way. The consultation document does not provide sufficient information about the operation of the ICO for respondents to make a judgement about possible "legislative or other measures". However, transparency could be improved through scrutiny by the public via representative organisations and Parliament rather than by the government of the day.

Q5.4.5. Please share your views on any particular evidence or information the ICO ought to publish to form a strong basis for evaluating how it is discharging its functions, including with respect to its new duties outlined in section 5.4.

Q5.4.6. To what extent do you agree with the proposal to empower the DCMS Secretary of State to initiate an independent review of the ICO's activities and performance?
○ Strongly disagree

Q5.4.6a. Please explain your answer, and provide supporting evidence where possible.

JAAG believes that every public body must be subject to scrutiny. However, such scrutiny must be and be seen to be completely free from political influence. We believe that the ICO performs its functions on behalf of citizens very well, within the resources available, and see no reason for it to be reviewed at this time.

Q5.4.7. Please share your views on what, if any, criteria ought to be used to establish a threshold for the ICO's performance below which the Government may initiate an independent review.

JAAG believes that any review must be fully independent, and therefore that it is Parliament itself that should call for a review and control this process of accountability, rather than the Government of the day.

5.5. Codes of Practice and Guidance

Q5.5.1. To what extent do you agree with the proposal to oblige the ICO to undertake and publish impact assessments when developing codes of practice, and complex or novel guidance?
○ Strongly disagree

Q5.5.1a. Please explain your answer, and provide supporting evidence where possible.

The guidance and codes of practice reflect best practice to meet legal requirements. If this requires organisations to go further than their current efforts, that is a good thing for society and aids organisations in meeting their legal requirements. It is exactly what a regulator should be doing and is not something to be avoided.
This is not the type of situation where impact assessments are appropriate. Instead, impact assessments should be used when organisations are investigating the potential risks, harms, effects etc. of their business proposals. The regulator is part of the system to ensure accountability of these organisations; it should not itself be constrained from doing its job properly, but should be properly resourced in order that the accountability mechanism can be effective.

Q5.5.2. 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 disagree

Q5.5.2a. Please explain your answer, and provide supporting evidence where possible.

JAAG believes that the Secretary of State should not have the power to make this a requirement, but that in many cases it would be a good idea for ICO to consult such parties (as they already do). Rather, resourcing to the ICO should be increased so that ICO can refine guidance in the light of feedback. The ICO can be trusted to involve experts where appropriate in drafting such guidance. JAAG considers it of vital importance that ICO should not be constrained either in the selection of experts or in the extent of their influence.

Q5.5.3. To what extent do you agree with the proposal to give the Secretary of State a parallel provision to that afforded to Houses of Parliament in Section 125(3) of the Data Protection Act 2018 in the approval of codes of practice, and complex and novel guidance?
○ Strongly disagree

Q5.5.3a. Please explain your answer, and provide supporting evidence where possible.

JAAG is very concerned that this proposal might introduce the risk of inappropriate political influence over codes of practice and complex and novel guidance.

Q5.5.4. The proposals under section 5.5. would apply to the ICO's codes of practice, and complex or novel guidance only. To what extent do you think these proposals should apply to a broader set of the ICO's regulatory products?
○ Strongly disagree

Q5.5.4a. Please explain your answer, and provide supporting evidence where possible.

We do not consider that these proposals should apply to any regulatory products.

Q5.5.5. Should the ICO be required to undertake and publish an impact assessment on each and every guidance product?
○ No

Q5.5.5a. Please explain your answer, and provide supporting evidence where possible.

This seems totally inappropriate for, say, a user manual containing guidance. It may be appropriate to undertake such an assessment internally if that manual ever had to be modified in the future. Such an analysis would help estimate the costs and risks of the change. However, it would be a detailed piece of work and not relevant to a wider readership: it would therefore not need to be published. A requirement to undertake and publish an IA would impede the work of the ICO and be a waste of time and resources.

5.6. Complaints

Q5.6.1. To what extent do you agree that the ICO would benefit from a more proportionate regulatory approach to data protection complaints?
○ Strongly disagree

Q5.6.1a. Please explain your answer, and provide supporting evidence where possible.

JAAG firmly believes that any ‘proportional’ regulatory approach should not in any case permit the ICO to disregard any data protection complaint.

Q5.6.2. To what extent do you agree with the proposal to introduce a requirement for the complainant to attempt to resolve their complaint directly with the relevant data controller prior to lodging a complaint with the ICO (with guidance and exemptions)?
○ Strongly disagree

Q5.6.2a. Please explain your answer, and provide supporting evidence where possible.

JAAG does not believe it is necessary to make this a requirement because if the data controller has a straightforward and accessible process for resolving complaints, citizens will in any case take this approach, if appropriate. However, if a citizen finds the data controller's complaints mechanism opaque or obstructive, then their only recourse is to take their complaint straight to the ICO.

Q5.6.3. To what extent do you agree with the proposal to require data controllers to have a simple and transparent complaints-handling process to deal with data subjects' complaints?
○ Strongly agree

Q5.6.3a. Please explain your answer, and provide supporting evidence where possible.

This is a good idea. As mentioned in the proposal, it would be part of a good privacy management programme.

Q5.6.3b. Please also indicate what categories of data controllers, if any, you would expect to be exempt from such a requirement.

None beyond what is currently allowed for security reasons.

Q5.6.4. To what extent do you agree with the proposal to set out in legislation the criteria that the ICO can use to determine whether to pursue a complaint in order to provide clarity and enable the ICO to take a more risk-based and proportionate approach to complaints?
○ Strongly disagree

Q5.6.4a. Please explain your answer, and provide supporting evidence where possible.

There is sufficient flexibility in the current legislation and instead this proposal seems likely to further disempower individuals.

5.7. Enforcement Powers

Q5.7.1. To what extent do you agree that current enforcement provisions are broadly fit for purpose and that the ICO has the appropriate tools to both promote compliance and to impose robust, proportionate and dissuasive sanctions where necessary?
○ Somewhat agree

Q5.7.1a. Please explain your answer, and provide supporting evidence where possible.

This is dependent on ICO maintaining their independence, and being given sufficient resource for personnel etc. to carry out the enforcement and to check compliance, etc.

Q5.7.2. To what extent do you agree with the proposal to introduce a new power to allow the ICO to commission technical reports to inform investigations?
○ Strongly agree

Q5.7.2a. Please explain your answer, and provide supporting evidence where possible, including:
Q5.7.2a1. Whether there are any other risks or benefits you can see in this proposal

This seems a good idea, as it utilises specialist and domain-specific knowledge and frees up ICO resource for other tasks.

Q5.7.2a2. If you foresee any risks, what safeguards should be put in place

CO should be fully free to choose whom they use or engage in this process: it is important that the independence of ICO from government is maintained.

Q5.7.3. Who should bear the cost of the technical reports: the organisation (provided due regard is made to their financial circumstances) or the ICO?

The organisation, if data protection irregularities are found. Otherwise, this could be funded out of penalties imposed (either to this organisation or others).

Q5.7.4. If the organisation is to pay, what would an appropriate threshold be for exempting them from paying this cost?

The threshold should depend upon the degree of data protection irregularities found, being much higher if there are greater irregularities. Ultimately, the upper bound could be the bound of fines imposable for GDPR non-compliance.

Q5.7.5. To what extent do you agree with what the government is considering in relation to introducing a power which explicitly allows the ICO to be able to compel witnesses to answer questions at interview in the course of an investigation?
○ Strongly agree

Q5.7.5a. Please explain your answer, and provide supporting evidence where possible. In particular, please give your views on any benefits or risks you envisage and what measures could mitigate these risks.

There is a risk that employees might be put in a difficult position for testifying against an organisation, so some means of protection should be given for them against subsequent maltreatment by the organisation or prior pressure by the organisation.

Q5.7.6. To what extent do you agree with extending the proposed power to compel a witness to attend an interview to explicitly allow the ICO to be able to compel witnesses to answer questions in the course of an investigation?
○ Strongly agree

Q5.7.6a. Please explain your answer, and provide supporting evidence where possible. In particular, please give your views on:

Q5.7.6a1. Any benefits or risks you envisage

There is a need to avoid pressure for witnesses to lie, which may arise for a variety of reasons (e.g. fear of self-incrimination, fear of losing their job, fear of incriminating colleagues, etc.)

Q5.7.6a2. What, if any, additional safeguards should be considered?

Anonymisation and redaction of some information shared with the organisation would help, even though the ICO can see it.

Q5.7.7. To what extent do you agree with the proposal to amend the statutory deadline for the ICO to issue a penalty following a Notice of Intent in order to remove unnecessary deadlines on the investigations process?
○ Strongly agree

Q5.7.7a. Please explain your answer, and provide supporting evidence where possible.

This seems reasonable for the reasons given in the proposal.

Q5.7.8. To what extent do you agree with the proposal to include a 'stop-the-clock' mechanism if the requested information is not provided on time?
○ Strongly agree

Q5.7.8a. Please explain your answer, and provide supporting evidence where possible.

This seems reasonable for the reasons given in the proposal.

Q5.7.9. To what extent do you agree with the proposal to require the ICO to set out to the relevant data controller(s) at the beginning of an investigation the anticipated timelines for phases of its investigation?
○ Somewhat disagree

Q5.7.9a. Please explain your answer, and provide supporting evidence where possible.

It seems to involve extra work and constraints, in situations which are difficult to predict in advance how much investigation will be required. It would be better to resource the ICO adequately so that it is feasible for them to conduct investigations in a timely manner.

5.8. Biometrics Commissioner and Surveillance Camera Commissioner

Q5.8.1. To what extent do you agree that the oversight framework for the police's use of biometrics and overt surveillance, which currently includes the Biometrics Commissioner, the Surveillance Camera Commissioner and the ICO, could be simplified?

Q5.8.1a. Please explain your answer, and provide supporting evidence where possible.

Q5.8.2. To what extent do you agree that the functions of the Biometrics Commissioner and the Surveillance Camera Commissioner should be absorbed under a single oversight function exercised by the ICO?

Q5.8.2a. Please explain your answer, and provide supporting evidence where possible.

5.9. Further Questions

Q5.9.1. In your view, which, if any, of the proposals in 'Reform of the Information Commissioner's Office' would impact on people who identify with the protected characteristics under the Equality Act 2010 (i.e. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation)?

The proposal to downplay individual data protection complaints would have an especially bad impact on people who identify with the protected characteristics under the Equality Act 2010.

Q5.9.2. In addition to any of the reforms already proposed in 'Reform of the Information Commissioner's Office' (or elsewhere in the consultation), what other reforms do you think would be helpful to improve the effectiveness of the ICO?

Maintain its independence, and properly resource the ICO so that it can do its job effectively and in addition, allow it to keep the money it raises from fines.

Note: this question is only online, not in the pdf version.

Q5.9.2a. End of chapter Q. Do you have any general comments about this chapter not yet captured by your responses to the questions above?

Throughout the document we see the influence of corporate lobbying (including via CIPL), to the extent that the majority of proposals seem directly or indirectly to help business interests at the expense of individual data protection rights. The document proposes that four of the seven key principles of the UK GDPR (Lawfulness, fairness and transparency; Purpose limitation; Data minimisation) are severely weakened and a fifth, accountability, redefined in such a way as to reduce individual data rights and key protections.

It is JAAG's considered view that this proposal will not even necessarily help business interests. As the ICO has pointed out, high data protection can be a business advantage. Furthermore the EU's adequacy decision for the UK would come severely under threat, threatening business interests and efficiency.

Note: this section of questions is only online and not in pdf; meaning that having worked through the pdf consultation you are not prepared for this set of questions.

Chapter 6

Q6.1.1. What compliance activities does your business currently undertake as a result of the UK GDPR and DPA? (please tick all that apply)

Q6.1.1a. If you selected 'Other' please provide more details

JAAG has severe reservations about the basis and conduct of the 'Analysis of expected impact' relating to this consultation. It has so many shortcomings as to be unworthy of the name ‘impact assessment’. JAAG will be happy to meet with you to go through these in detail.

Q6.1.1b. What do these compliance activities cost your organisation in time and money?

Q6.1.2. We would like to understand more about how (if at all) your organisation would be affected by the measures outlined in the consultation, specifically:
Q6.1.2a. What compliance activities would change as a result of the measures?
Q6.1.2b. What other impacts would the proposed measures have on your organisation?

Q6.1.3. How (if at all) would the proposed measures affect your organisation’s collection, use or processing of data?

Q6.1.4. We would like to understand more about how (if at all) international data transfers your organisation carries out would be affected by the proposed measures, specifically: What is your current reliance on and opinion of alternative transfer mechanisms?
Q6.1.4a. (For businesses/organisations) What impacts on your organisation do you expect from the proposed measures?