Written evidence submitted by:

British and Irish Law, Education and Technology Association (BILETA)

Data: A new direction inquiry (DCMS)

Prepared on behalf of the British Irish Law, Education and Technology Association (BILETA) by Dr Edina Harbinja, Dr Subhajit Basu, Dr Aysem Diker Vanberg, Dr Orla Lynsky, Dr Karen Mc Cullagh, Dr Henry Pearce, Dr Felipe Romero – Moreno, Gavin Sutter

The British and Irish Law Education Technology Association (BILETA) was formed in April 1986 to promote, develop and communicate high-quality research and knowledge on technology law and policy to organisations, governments, professionals, students and the public. BILETA also promotes the use of and research into technology at all stages of education. The present inquiry raises technological, economic and legal challenges that our membership explores in their research. As such, we believe that our contribution will add to the public discourse and the inquiry on the future of UK data protection law.

Chapter 1

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?*

A: Somewhat agree. The research sector is indeed an important one in the UK, and certainly legal clarity helps in facilitating that. Whether the present situation requires a specific legal change, however, as opposed to better official guidance from the ICO should be considered rather than simply rushing to 'more law' as a default. Care must also be taken to limit this to clarification, rather than prioritising the supposed needs of research ahead of personal information privacy.

One aspect in which new legislation might be helpful would be in distinguishing between legitimate, public-interest research and the purely commercial. For example, the Astrazeneca Covid-19 vaccination was a primarily publicly-funded[1]project with a clear public interest: bringing an end to the pandemic. Similar could be argued for a small university spin-out company. While it is imperative that such public interest work be facilitated where reasonably possible, the case for changing the law to make it easier to reduce data privacy concerns in commercial research which will be of primary benefit chiefly to the business interests involved is simply not a credible premise.

[1] A reported mere 3% of the overall budget for its development came from private sources; see, for instance: https://www.theguardian.com/science/2021/apr/15/oxfordastrazeneca-covid-vaccine-research-was-97-publicly-funded

Question 1.2.2 To what extent do you agree that creating a statutory definition of 'scientific research' would result in greater clarity for researchers?

Somewhat agree.

Clarification of what constitutes legitimate research could be helpful, however again it would be equally useful to incorporate a public interest criteria which made a clear distinction between academic research in the public interest, and that which is purely for the economic benefit of private individuals. We acknowledge that these could overlap, but it would be useful to distinigush cases where the former of the latter is a primary purpose.

Question 1.2.3 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?

This definition is a reasonable basis to begin with. The inclusion of "privately funded" in the definition is cause for concern from point of view that research exemptions should, where there is any potential for data privacy invasions (i.e. a lack of guaranteed, certain anonymity in the data), be very carefully weighed up in order to assess the level of data privacy infringement possible against data subject consent. Where any doubt exists, subject consent should always be the default position. It is clear from both the tone of the consultation document and the government's various policy comments in this area post-Brexit that there is an agenda to move away from the GDPR's balancing considerations between individual data privacy in order to permit greater financial exploitation of data, either in and of itself, or as a result of research and development using the data. Purely commercial, for-profit research is simply insufficient justification for an exception to the consent principle.

An ICO-led 'code of conduct' for the research sector – taking into account the differences in private and public sector / public interest research programmes - would be a welcome development. This would perhaps be of more practical benefit.

Question 1.2.4 To what extent do you agree that identifying a lawful ground for personal data processing for research purposes creates barriers for researchers?

Strongly disagree.

I have seen no clear evidence of a 'chilling effect' on research caused by data privacy laws, certainly nothing that could not be solved by clear, practical guidance from the ICO.

Question 1.2.5 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 [sic] *GDPR as a lawful ground would support researchers to select the best lawful ground for processing?*

Somewhat agree.

Clarification by means of ICO advice of the existing position for the essential public interest research done by UK universities would be welcome, providing that this does not erode the essential protection given the data subject by the consent principle. It is also important to consider to what extent this research can be 'gamed' by commercial interests and actors.

Question 1.2.6 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.

This would depend entirely on what is meant by a "new…ground for research", and the nature of any proposed safeguards. The existing law under the GDPR is sufficient to cover a wide range of research; it rather seems that all that could be gained by introducing new grounds (as distinct from clarification of the existing position) would be to facilitate mission creep and a gradual erosion of the existing protections for personal data.

Question 1.2.7. What safeguards should be built into a legal ground for research?

The research in question must have a clear and demonstrable public interest basis. Mere commercial benefit should not be sufficient for this. This would not necessarily shut out the private sector, however, private sector involvement should be subject to strict conditions, e.g. a novel medical development arising as a result of such research could be subject to significant public interest restrictions preventing it from being exploited solely or primarily for private gain.

Personal data should be collected in conditions of anonymity. For example, statistical information about an individual's Covid status and vaccine take-up (which vaccine, whether subsequently infected, *et cetera*) could be collected and entered into a research database at time of treatment, as distinct from provision of access to full or partial NHS health records.

The current 'best-practice' position – that where an individual could potentially be identified from notionally anonymized data (i.e. anonymity is not completely guaranteed) must be treated as personal data and subject to all requirements including consent – should be adhered to. This could *perhaps* be subject to a public interest exemption where there is a clear and demonstrable public interest in developing a new medical or other technology which will be made available via a non-profit arrangement (as opposed to on the 'free market') that can reasonably be concluded to outweigh the privacy interests of a specific individual. The researcher would need to be in a position to demonstrate that a specific individual's data (of an aggregate of inviduals' data) is indeed necessary to the study; merely helping fill out the sample size to a sufficient level to meet a set margin of error would not be sufficient here.

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 with this as a policy direction.

This is a leading question. It would obviously make things much easier for researchers if they could - as is the subtext of this question – abandon the requirement of informed consent inherent in the GDPR's data processing rules in favour of a more general, amorphous notion of consent. However, to do so as a general approach would represent an erosion of data subject rights which is unwelcome and should not be permitted. Of course, this should be subject to the existing 'necessity' exemptions, including the vital interests of the data subject.

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 agree.

Clarification is always helpful, however there is no credible reason why such clarification could not be made via official advice from the ICO, as distinct from legal change.

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.

The proposed exception would represent a very significant step away from the GDPR's requirement of informed consent, and is dangerously overbroad. An 'emergency public interest' criterion would be an improvement if strictly applied, but it is difficult to imagine a situation where credible research would begin without the knowledge that there may arise a need to apply a new usage *and* it be extremely difficult to The idea that the government might, in all but virtually uniquely unforeseeable circumstances, regard diminishing the requirement of individual consent (subject to the existing restrictions in the GDPR) in favour of unspecified "research interests", public or private, is at best concerning. Again, "a research purpose" is far too wide a category to allow for proper, informed consent to be given.

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

Were the government to make such an ill-advised exception, it should be subject to the tightest possible requirements of an overriding public interest amounting to a pressing social need that unequivocally can be said to outweigh an individual's interest in autonomous control over their own, personal data in the circumstances. Of course, where anonymity can be guaranteed at point of collection and going forwards (avoiding identification through profiling), that would already be permitted.

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

Somewhat disagree.

The GDPR list is well considered; the appropriate place for clarification is, again, in official advice from the ICO and not through tinkering with the law in a manner which will, almost inevitably, reduce its effectiveness as regards the protection of personal information privacy.

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.

The legislative text is not the ideal place for such clarification, ICO official advice would be preferable, and more easily updated as required.

A potential public interest exemption *may* be worth further exploration, but it should only be permitted on the narrowest of grounds, from an exhaustive list of circumstances provided in the legislation. Any such law should be subject to the requirement that it be clearly demonstrable that the public interest in the certain benefits of the research outweighs the public interest in protecting the data privacy of the individual data subjects concerned.

It is vital that any such decision be made by an authority which is not part of government. For example, it is far from fanciful to imagine a government decision to sell off NHS patient data in order to help fund the health service. Such a move should never be permitted under any such 'public interest' exemption.

Where any public interest exemption is to be applied, it should be subject to the prior approval of an independent regulator before it is applied.

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

Strongly disagree.

The law here is already sufficiently clear under GDPR standards. Insofar as any further clarification is truly necessary, it can readily be achieved via official advice from the ICO. The only real advantage to government from enshrining this in law would be for a government intent on eroding data subjects' rights in favour of the financial interests of data controllers.

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?

Strongly disagree.

The GDPR position is already significantly clear on this grounds. Again, there is an undertone in government discussion on this point which suggests that "clarification" is a euphemism for the adoption of lower standards of personal information privacy post-Brexit than UK citizens enjoyed prior to that.

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.

It is abundantly clear from this question alone (as well as the general tone of government communications on this matter) that the present executive is pushing a policy of diminishing individual autonomy *viz-a-vis* the right to information privacy. It is simply unacceptable that a public, private or otherwise commercial entity could be permitted to exploit an identifiable data subject's personal information absent both consent *and* being able to demonstrate an overriding public interest. There is simply no argument in favour of such a policy save that which favours financial benefit to organisations over individual autonomy, and that is not a credible basis on which to make such a change in law in a state which proclaims itself a human rights respecting democracy.

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.

a. Reporting of criminal acts or safeguarding concerns to appropriate authorities

Reporting criminal acts is uncontroversial, however this will have to be subject to the balancing test in the context that the subject seeks to exercise their 'right to be forgotten'. See, for instance, the judgement of the then Mr Justice Warby in *NT1 & NT2 v Google* [2018] EWHC 799 (QB), in which the entitlement to the right varied between the two claimants, based on the apparent need of society to be forewarned about their individual, criminal records.

b. Delivering statutory public communications and public health and safety messages by non-public bodies

Any passing of personal data held by public bodies to private entities must only be done where specifically necessary, and it is disappointing in the extreme that any UK government would be so cavalier as to not require a balancing test here.

c. Monitoring, detecting or correcting bias in relation to developing AI systems (see section 1.5 for further details)

Where any such activity is truly necessary, meeting the balance test will not be a hardship. The test provides an important, filtering function that must not be abandoned.

d. Using audience measurement cookies or similar technologies to improve web pages that are frequently visited by service users

As instances of invasive, aggressive online data harvesting activities rise exponentially, it would be irresponsible in the extreme to diminish existing legal protections for personal information. Recent government promotion of its agenda being styled as 'getting rid of annoying cookie warnings' is sadly indicative of an executive which not only values business interests over and above those of its citizens, but is intent on enshrining such a value system in law.

A preferable policy would be to further increase, not diminish, personal information protection here – such as by requiring detailed, nuanced user consent to cookies, allowing an individual (as is currently best-practice) to choose between different types of information to be collected (functional cookies vs advertising cookies) or between website provider cookies and third-party cookies. Browser controls are far too binary in the options they offer

to be able to achieve this, and also play to a false narrative that an individual will have the same cookie preferences in relation to any and all websites.

Data privacy is an important – and, in the online world, increasingly fundamental – right, and there simply can never be a credible argument in favour of diminishing that right in order to facilitate financial gain. Removing any consideration for user rights as a balancing factor in this context is an unjustifiable attempt to put profit before personal privacy.

e. Improving or reviewing an organisation's system or network security

Under no circumstances should the interests of the organisation be automatically placed over and above those of the individual by default – which is, in practical effect, what this proposal would lead to.

f. Improving the safety of a product or service that the organisation provides or delivers

If processing can genuinely be proven to improve safety, then this should not need a further change with the law as it could clearly come within the necessity criterion if it genuinely offers a significant safety benefit to the user. Otherwise, consent should be required as normal.

g. De-identifying personal data through pseudonymisation or anonymisation to improve data security

Pseudonymising data should already be being done where appropriate best-practice; the proposed exception offers nothing here. If data is genuinely anonymised (i.e. the organisation can *guarantee* that it cannot be reverse engineered either alone or when added to other profiling information), then the data controller is already free to do as they please as under the current legal position it is not personal data.

h. Using personal data for internal research and development purposes, or business innovation purposes aimed at improving services for customers

The primary benefit – and the real motivation here – is not one of altruism. The company benefits in the market from 'service improvements'. It being the case that the company is thus, in the last instance, simply acting in its own best interests in the competitive marketplace, there is no reason to facilitate this over and above the rights of the data subject.

i. Managing or maintaining a database to ensure that records of individuals are accurate and up to date, and to avoid unnecessary duplication

This criterion makes little or no sense in this context. The data collector is required under existing law to take such measures in order to maintain the accuracy and integrity of data. There is no obvious reason why it would benefit the data controller to not have to consider data subjects' interests here when the whole point of the legal obligation to undertake such activities is to protect those rights.

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

None. There is no compelling argument for any such change to the GDPR in the first instance.

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?

The enhanced level of protection for children's personal data enshrined in the GDPR should be maintained at all costs.

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 disagree**

UK wants to be at the forefront of the AI and data revolution. The National AI Strategy, published in September 2021, aim to invest and plan for the long-term needs of the AI ecosystem and support an AI-enabled economy. However, AI has become a problematic concept in policy, particularly from the 'fairness' perspective. There are risks that algorithmic decisions may be mistaken or discriminatory. Data should be used to tackle bias and exclusion in society. Better data will tell us how different groups are doing and identify potentially vulnerable groups more quickly. However, we also know that algorithms based on data inputs are not always neutral. AI systems learn to make decisions based on training data, including biased human decisions or reflecting historical or social inequities, even if sensitive variables such as gender, race, or sexual orientation are removed. In August 2020, the Court of Appeal in R Bridges v CC South Wales Police [2020] EWCA Civ 1058 found that South Wales Police's use of facial recognition technology breaches privacy rights, data protection laws and equality laws. A-level grading controversy in Summer 2020 also demonstrated how difficult it could be, even with the best intentions. In the UK, there is currently no AI-specific legislation. The obligations of non-discrimination set out in Data Protection Act 2018 and Equality Act 2010 are not specific to AI but are issues relevant for any AI implementations that use personal data to make decisions, predictions, or inferences about individuals. However, data protection is not a complete – nor necessarily even a particularly satisfactory – solution to the legal issues raised by AI and machine learning technologies when it comes to fairness[2].

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?

○ **Neither agree nor disagree**

The concept of fair processing is set out under Article 5(1)(a), which covers several processing practices. However, fairness is a subjective and contextual concept that is influenced by several social, cultural and legal factors and is magnified in the AI context. The duty of fairness is a pre-condition for lawful processing of data; however, it is contentious if data protection law adequately provides explicit and well-defined safeguards for the concept; for example, in R Bridges v CC South Wales Police, South Wales police had not considered the risk of discrimination when using automated facial recognition. Articles 13(2)(f), 14(2)(g), 15(1)(h), and 22 supports a right to explanation but does not elaborate much beyond that point[1]. A European Parliament report on the fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement, European Parliament expressed that "because of the data sets and algorithmic systems used when making assessments and predictions at the different stages of data processing, big data may result not only in infringements of the fundamental rights of individuals but also in differential

[2] Veale M, Binns R, Edwards L. 2018 Algorithms that remember: model inversion attacks and data protection law. Phil. Trans. R. Soc. A 376, 20180083.

treatment of and indirect discrimination against groups of people with similar characteristics, particularly concerning fairness and equality of opportunities for access to education and employment, when recruiting or assessing individuals or when determining the new consumer habits of social media users."[3] Further, the data protection law only covers personal data, not the ML models themselves.

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.

ICO has looked at the interplay between data protection principles and discrimination. ICO and Equality and Human Rights Commission should play a pivotal role; however, ICO and Equality and Human Rights Commission have limited financial and human resources to take effective action. It is also not apparent if ICO has the necessary expertise to detect or evaluate algorithmic discrimination. The anti-discrimination legislative framework, notably through the Equality Act 2010, offers individuals protection from discrimination, and it should, in principle, protect an individual in case of an automated decision-making system from discrimination. However, anti-discrimination law does not address the possibility that prediction may prove to be wrong in a particular case. A legal 'gap analysis' should be undertaken to understand how AI systems can be regulated to protect from and prevent breaches of human rights and to identify whether there is a need for reform. 'Fairness' could be effectively embedded if the organisations that deploy AI and algorithms should be compelled to conduct and publish Algorithmic Impact Assessments, similar to Data Protection Impact Assessments, which demonstrate that the potential for the technology to discriminate has been assessed and minimised.[4]

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**
ICO appears to place significant weight on the importance of the fairness principle to regulate machine learning systems appropriately. However, the fairness principle remains somewhat of a nebulous concept, and its relationship with the more accountability principle-orientated obligations on those processing personal data remains hard to characterise in a precise manner. In our view, there is a need to bridge the gap between the abstract formulation of the fairness principle in data protection and fairness metrics for making AI systems fair. Combining data protection and equality law may provide new opportunities for developing fair algorithms. ICO could be entrusted to initiate a dialogue with other relevant authorities to develop a much more robust framework for fairness

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

○ **Somewhat agree**
We agree that insufficient training data is another cause of algorithmic bias; hence, better access to data is needed. However, the government's aim for 'innovation-friendly regulation' seems to place greater emphasis on 'effective mechanism for communicating government's strategic priorities and a 'deregulatory approach overall' than it does on genuinely supporting effective coordination to clarify and enforce the law through collaborative initiatives. An

[3] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf
[4] See https://ainowinstitute.org/aiareport2018.pdf

approach focused on avoiding and mitigating the potential risks of personal processing data is a necessary element of the responsible innovation of AI. The process of more 'freely sharing' of data should be value-oriented and should adopt a precautionary approach based on appropriate risk prevention and mitigation measures. . It should not become a 'race to the bottom.' ICO should be provided with sufficient resources to support and monitor programmes of AI developers. Awareness of risk is not a barrier to innovation but rather an enabler

Q1.5.6. When developing and deploying AI, do you experience issues with identifying an initial lawful ground? Please explain your answer, and provide supporting evidence where possible.

The development and use of AI should be done safely, effectively, and ethically acceptable. We disagree with the government that the current situation "creates doubt and uncertainty which may lead to friction and a potential reduction in innovation (para 83)". Any deregulatory approach would be counterproductive as it will reduce public trust in the system. Downplaying the role of law carries risks of increasingly implicating AI as a 'legal opportunity'. It is paramount that the design and governance of AI be accountable, fair and transparent. Hence before the development takes place, due consideration should be given to both the ethical concerns of the "should vs should not" in the development of AI solutions and the more legislative regulations of "could vs could not".

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

ICO provides advice and guidance to organisations on interpreting the UK GDPR "on the re-use" of personal data. The government must recognise the need for a range of measures, including transparency of processing, raising the public's awareness of how personal data may be used, and adopting robust measures by organisations to mitigate the risks. While this may be viewed as creating tension between the use of AI systems and data protection law, since it is not always possible to predict what data elements may be relevant to the objective of the system, the principle in itself does not limit the processing of data by way of reference to a specific volume or set of data elements—it refers to what is "necessary" for the processing. It is a delicate balance between the benefits of processing data and respecting people's privacy concerns within the scope of the principles and definitions provided. This debate over the interpretation of the data re-use regulation has been ongoing; even though the GDPR has provided some legal clarity, it has not solved the critical problem of informed consent sufficiently.

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

UK GDPR exempts research from the principles of storage limitation and purpose limitation to allow researchers to further process personal data beyond the purposes for which they were first collected. It also provides some exceptions for research data when the necessary safeguards are in place and applies only to personal or special categories data, not to all research data in general, nor anonymised data. Hence it is unlikely that AI developers are facing any significant problems.

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

○ **Somewhat agree**

We agree personal data may be needed to monitor, detect and correct bias in AI systems, and it makes sense to include processing personal data for this purpose in the list of processing that constitutes a "legitimate interest" in Article 6(1)(f) for which the balancing test is not required. It is effectively grounded in risk-based organisational accountability. However, it is not clear how the government is proposing to balance the risk between the legitimate interest of an organisation to process the data for this purpose and the right of an individual in this specific context. Hence further explanation should therefore need to be provided to ensure consistency in the interpretation and application of the provision. For example, in its guidance on AI and Data Protection, ICO provides an auditing framework for AI compliance that includes a roadmap for individuals designing, building and implementing AI systems that are heavily based on risk assessments[5]. We propose that organisations should, under these circumstances, provide individuals with an online contact form, with an email/postal address to which any objection may be sent, via an opt-out option, or via a setting allowing the data subject to effectively "self-serve" by turning off any legitimate interests-based data processing.

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?

○ **Strongly agree**

The Data Protection Act 2018 provides the processing of personal data where it is for equality of opportunity or treatment. The proposal is to use data to eliminate bias in AI systems or to create a new lawful basis covering the use of special category data for monitoring, detecting, and correcting bias in AI systems. The sensitivity of the data heightens risks; hence, to ensure that data processing for equal opportunities and reduce bias in AI systems, a new condition within Schedule 1 that specifically addresses the processing of sensitive personal data for AI systems should be developed, and it needs to be a lot more prescriptive, further ICO should be mandated to continue to provide sector-specific guidance in this area. However, the proposal contradicts the government's stated goal to ensure that the rules are not set by reference to a particular technology but rather are adaptable and dynamic that can be applied to new and emerging technologies as they develop.

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

○ **Strongly agree**

We agree that a new condition within Schedule 1 that specifically addresses the processing of sensitive personal data for AI systems should be developed, even though organisations may be able to rely on an existing derogation in the Data Protection Act 2018 the derogation in Para 8 of Schedule 1 refers to identifying or keeping under review the existence or absence of equality of opportunity. A separate condition would be to bring clarity, provide adequate safeguards, and reduce compliance and enforcement deficit.

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

The principle of transparency and accountability sits at the heart of public trust in AI systems. Hence to develop a trustworthy AI system, there is a need to establish a regulatory framework for data protection to ensure transparency, bias/fairness, risk assessment and stiff penalty for non-compliance. Organisations should be incentivised to guarantee greater transparency in using AI systems through a comprehensive and systematic mapping of the different ways in which these systems developed and deployed. This aim for greater transparency should

[5] ICO Guidance on AI and Data Protection, July 2020

complement and work alongside the data protection provisions, which is only a meaningful legal instrument supporting equality where appropriate levels of transparency exist. Algorithmic impact assessments could be part of this regulatory strategy as it provides the opportunity to evaluate the development and adoption of an AI system.

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

○ **Somewhat agree**
We welcome the inclusion of Article 22 in the consultation; however, we disagree with removing Article 22 of the UK GDPR, as recommended by the Taskforce on Innovation, Growth and Regulatory Reform, which gives people "the right not to be subject to a decision based solely on automated processing, including profiling." Although it is a potentially significant right, it does not seem to apply very frequently in practice because many AI-driven decisions about people fall outside the scope of the provision. It is not easy to see how abolishing the provision would seriously increase innovation. We agree that there is a need to reassess Article 22 to consider whether it would permit automated decision-making and remove the human review of algorithmic decisions without expanding automated processing and profiling for commercial interest. The term 'similarly significant' is ambiguous and needs interpretation. It has been contended that Article 22 has limited applicability since it only applies to 'decisions based solely on automated processing' when there is even minimal human intervention included in the algorithmic decision-making process, safeguards indicated under Article 22(3). There is very little detail in the consultation on protecting the issues that human oversight is meant to address. Data subjects have a right to understand how decisions are made, and there needs to be an adequate and effective redress mechanism (while the EU is taking an opposite direction).

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

○ **Yes**
Development of an 'external oversight mechanism' and make the human intervention much more meaningful.

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

○ **Neither agree nor disagree**
The complexity of algorithms can make it challenging to understand the rationale behind an automated decision. We accept that Article 22 does not always provide meaningful safeguards regarding uncertainties around its operation, terminology, and narrow scope. We agree that article 22 is not sufficiently future-proofed to be practical because it forces the organisation to use less accurate AI systems that fail to protect individuals from unfair decisions. Further, there are technical limitations that create problems concerning the scope and applicability of the provisions. However, as we said before, Article 22 should not be abolished; instead, it should be reformed to ensure that the transparency requirements are strengthened, due process and an appropriate scrutiny mechanism is always followed. There seems to be a tendency to overlook law in UK's AI policy development[6].

[6] Earlier this year Dutch government resigned over a scandal where the government had used an algorithm to predict who is likely to wrongly claim child benefits. Without any evidence of fraud, the tax authority forced 26,000 parents — singling out parents of dual nationalities and ethnic minorities — to pay back tens of thousands of

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**

Q1.5.18. 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.

Algorithmic profiling may result in discriminatory outcomes. UK GDPR contains dedicated rules for algorithmic profiling; there are limits to applying data protection law in countering algorithmic profiling and the drawing of sensitive or discriminatory inferences. Data protection law may not be a good resource to challenge the problems of algorithmic profiling; however, as algorithmic deductions made about an individual are considered personal data; existing protections should be amended or extended to cope with new forms of discrimination emerging. We also think anti-discrimination laws may offer a more promising outcome.

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.

Fundamentally, the problem which the regulation must seek to solve is the problem of controlling undesirable risks to prevent harm. Data provides the building blocks for AI. Data protection framework affects the use of AI in at least four ways: limiting the collection and use of data, restricting automated decision-making, increasing compliance costs and risks, and providing a robust accountability framework. It has been argued persuasively that data protection framework (GDPR) lacks precise language as well as explicit and well-defined rights and safeguards against automated decision-making'[7] even if the entitlement to 'meaningful information is undeniably significant'[8], still it is the proper legislative framework to evaluate collective data-driven harms (probably together with the anti-discrimination laws). It is effective against manipulative, social control and indiscriminate surveillance practices. It is undeniable EU has been one step ahead as the EU Commission published the first draft of the Artificial Intelligence Regulation. This is a significant piece of legislation. It creates a regulatory ecosystem focussed on "high-risk" uses of AI (e.g. in employment, education and credit scoring settings), bans some manipulative uses of AI and requires transparency in other contexts. It is proposing to set up standards that would pave the way to the development of ethical technology. However, misplaced regulations have the potential to stifle innovation and derail the enormous potential benefits that AI can bring. We certainly do not want rules hastily put together as a knee-jerk response to a technology that is still developing.

euros to the tax authority without the right to appeal. https://www.politico.eu/article/europe-artificial-intelligence-blindspot-race-algorithmic-harm/

[7] Sandra Wachter, Brent Mittelstadt, Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, Volume 7, Issue 2, May 2017, Pages 76–99

[8] Andrew D Selbst, Julia Powles, Meaningful information and the right to explanation, *International Data Privacy Law*, Volume 7, Issue 4, November 2017, Pages 233–242

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?

○ **Neither agree nor disagree**

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

The proposal rightly points out that making determinations as to whether data are personal or anonymous can be very challenging and complex. The proposal is also correct to point out that the current threshold for determining whether data are either personal or anonymous is unclear. Pursuant to this, there is a clear need to clarify when and in what circumstances data will be legally anonymous.

However, of the two proposed solutions (i.e. 121.a and 121.b), neither is likely to drastically improve the current situation, though solution 121.a is the preferable of the two.

Incorporating Recital 26 of the UK GDPR onto the face of the legislation would create a concrete requirement that data controllers must take into account "all the means reasonably likely to be used" to (re)identify an individual, but the majority of data controllers who engage in anonymisation-related activities already deploy such an approach anyway. In any event this wording, whilst not unsensible, is vague, and does not provide much by way of substantive guidance re: when data are personal and when they are anonymous.

Option 121.b is a poor idea. If data are to only be legally anonymous when "it is impossible to re-identify the data subject", or if re-identification would require a disproportionate amount of time and effort, then very few types of data and information would ever meet this threshold. Whilst the use of such a standard may help to establish greater certainty in the law, it would also massively expand the concept of personal data, making data protection law potentially apply to an even wider range of information types than it does presently. This could have the effect of creating huge administrative burdens for data controllers.

The use of this approach could also lead to injustices, and harmful behaviours falling outside the scope of the law by way of legal technicalities. An individual whose data are at the heart of a de-anonymisation attack which requires "unreasonable time, effort, or resources' presumably would not, for example, be protected by the law, which would be completely illogical and contra to the aims of the legislation.

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

○ **Recital 26 of the UK GDPR**

○ Explanatory Report to the Modernised Convention 108+

○ N/A - legislation should not be amended

○ Other

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

Recital 26, for the reasons given above (i.e. in response to Q1.6.1).

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 agree**

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

This is a good idea. As is widely acknowledged in the literature pertaining to both data protection law and computer science, identity and anonymity are scalar concepts that not only like on a spectrum/continuum, but are highly context-dependent. Data that may "relate to" an individual in one context or in the possession of one data controller may not "relate to" anyone in another context or in the possession of another data controller, and this nuance should be expressly acknowledged in legislative wording.

As the proposal alludes to, incorporating the approach of *Breyer v Germany* into the wording of the legislation would not necessarily change the existing legal position in the UK. As has been acknowledged in the literature, UK case law relating to the notions of personal data, anonymity, and identifiability, has shown a trend of a steady move towards a context/risk-based approach to data categorisation (i.e. whether data are personal or anonymous).

However, over the last few decades, there has been judicial disagreement, and the path to the current (and absolutely correct) approach has not been smooth. So to safeguard and concretise the current approach, it should absolutely be confirmed in legislation that the question of whether data are anonymous is relative to the means available to the data controller to re-identify those data (as well as other contextual factors, such as who within an organisation has access to the data, the purposes for which the data are to be processed, the existence of any organisational/technical/security measures in place, and indeed the existence of any motivated intruders).

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.

Yes, there are a number of important and emerging areas in which the use of privacy by design (PBD) techniques would be beneficial (particularly in relation to public sector data handling and disclosure practices, including those relating to freedom of information), and there is a clear role to be played by the government in terms of encouraging and incentivising their use.

PBD-based approaches are especially useful in situations where problems are best solved by prevention rather than cure, where individual rights must be balanced against other competing interests, and where a problem is complex, dynamic, multifaceted and insusceptible to ex-post legal rules and remedies. Protecting individuals from harms associated with errant or nefarious uses of their personal data, whilst concurrently attempting to ensure that innovative uses of personal data are not unduly restricted, is a regulatory challenge possessing all of these characteristics.

At present, data protection law establishes a number of punitive sanctions for data controllers who breach their data protection obligations, and a number of remedies for individuals who suffer harm as a result. These may often be ineffective. As has been established in the literature, attempts to address privacy harms post-occurrence will often be ineffective (e.g. data protection rights and remedies, or even remedies from other areas of law, will unlikely be of much use to a data subject whose personal data have been leaked online, are "out there", and have come into the possession of nefarious parties, some of whom might be based in other jurisdictions and could not care less about what is said in UK law.)

The use of PBD approaches could have the potential to prevent data-protection and privacy-invasive harms arising in the first place (e.g. because data that have not been leaked in the first place cannot be used for harmful purposes). This will ultimately be to the benefit of all parties. For data controllers, the use of such approaches may limit their exposure to serious liability stemming from breaches of their data processing operations. For data subjects, an extra layer of safety and security for the processing of their personal data will be established. As highlighted elsewhere, the use of PBD techniques (such as data licensing schemes, and the use of techniques such as differential privacy) can be hugely beneficial in terms of increasing public trust in organisations (both private and public sector) handling and using their personal data (Pearce 2020).

That said, the government should also bear in mind research which has highlighted how the use of PBD techniques may, in some situations, have the potential to create negative privacy impacts (Veale, Binns, Ausloos 2018)

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

○ **Yes**

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.

The proposal is correct to highlight the potential of data intermediaries. These are services that may be extremely valuable, particular in terms of furthering open data initiatives and facilitating the re-use of public sector data. However, despite their potential to alleviate social, structural, and technical barriers to data usage and sharing, there are reasons as to why the development of many such services remain nascent. Namely because, as the proposal itself alludes to, there are concerns as to their trustworthiness of such services, and doubts and/or a lack of awareness as to their value and accountability. To this end, any suggestion that any service categorised as a "data intermediary" should in any way enjoy a "lighter touch" application of data protection rules, or an exemption to any such rules, should be resisted. These are services that should be bound by the same data protection rules as any other data controller, and they should not enjoy any special status. This is particularly the case given the highly sensitive nature that some services of this type may store/share etc. (e.g. health data, financial data etc.) The notion that an organisation or service (i.e. a data intermediary) which is designed to *increase* trust in, and facilitate, data sharing and re-usage, should be subject to a *lower* standard of legal rules than other data controllers is inherently contradictory.

A government approved accreditation scheme for data intermediaries may help to add confidence and grow trust in the use of these services and in data-sharing/re-use initiatives more generally. However, were such an initiative to be pursued, it is likely that concerns would arise in relation to fair competition (e.g. the possible perception of government-endorsed services being given competitive advantages over non-government-endorsed services, and user-lock in etc. or the selection process for government accreditation being non-transparent and/or corrupt) and privacy (e.g. concerns that data stored by government-endorsed services may in some situations be accessible by government bodies themselves). A rigorous auditing process for data intermediaries sounds like a good idea, but it is not at all clear how this would be achieved in a purely practical sense. Audits of this kind would presumably be the responsibility of the ICO, but in order for the ICO to take on such a role effectively its funding would likely have to be stepped-up and increased significantly.

Q.1.7.2. 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, whereby organisations share personal data without it being requested by the data subject?

The most obvious legal basis for such uses of personal data would be the "legitimate interests" ground for personal data processing. Exactly when and in what circumstances this ground would apply, and which/what types of data intermediary would be able to rely upon it, however, would depend entirely on context, and the nature of the intermediary service provided, and the personal data involved.

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)?

Any widening of the lawful grounds for personal data processing under Article 6 and Article 9 UK GDPR would potentially impact on people who identify with the protected characteristics under the Equality Act 2010. Personal data relating to any of these characteristics are highly sensitive, and their processing can result in extremely harmful consequences for affected persons. In particular, creating a new lawful ground for personal data processing for the sake of research, of widening the public interest as a ground for personal data processing, increases the possibility of such data being used for harmful purposes (i.e. because doing so will create more opportunities for data controllers to identify a legitimate way to process such data), and/or such data falling into the hands of nefarious parties who may themselves wish to turn the data to harmful purposes.

Chapter 2

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 agree. Accountability is a key element for a high standards data protection regime, both in the UK and internationally[9]. It is indeed desirable to have an accountability framework that features fewer prescriptive elements which are also more flexible, and more risk-based. However, the introduction of a privacy management programme on top of the current legal framework does not make things less prescriptive or more risk-based, it just adds red tape. Hence, any amendments to the current Data Protection Act 2018, the UK General Data Protection Regulation and the Privacy and Electronic Communications Regulations 2003 should be treated carefully as these changes could threaten the adequacy decisions for the UK. As noted by Lynskey, the changes proposed in the consultation document on the independence of ICO and the broader divergence from the fundamental rights dimension of data protection may be a cause for concern for the future of the UK's adequacy status[10].

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'?

Neither agree nor disagree. Organisations will benefit from being required to develop and implement a risk-based privacy management programme (PMP). However, we are concerned that developing and implementing a risk-based privacy management programme could create additional workload and additional costs for organisations. Most of the organisations have spent considerable time and effort in complying with the UK GDPR. Hence, any additional requirement may adversely affect small or medium-sized organisations, which do not have the financial means to develop and implement an efficient risk-based privacy programme. In this respect, as put forward by the ICO the Government should demonstrate whether the additional benefits of a PMP approach would outweigh the costs involved in making these changes[11]. Any PMP programme requirements will come on top of UK GDPR requirements, as they cannot replace domestic law and international standards on data protection. Moreover, the PMP will be quite burdensome for international organisations operating both in the EU and UK, as they will be required to comply with two different sets of standards. This may be a formidable disincentive to invest or even operate in the UK.

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. Individuals will benefit from organisations being required to implement a risk-based privacy management programme(PMP). However, these

[9] Information Commissioner's Office " Response to DCMS consultation " Data: a new direction" para. 43 p.39. <https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf > accessed 29 October 2021.

[10] Orla Lynskey "EU-UK Data Flows: Does the "New Direction" lead to "Essentially Equivalent" Protection?" Blogpost < https://dcubrexitinstitute.eu/2021/09/eu-uk-data-new-direction/> accessed 29 October 2021.

[11] Information Commissioner's Office " Response to DCMS consultation " Data: a new direction", para. 58, p. 42 <https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf> , accessed 29 October 2021.

programmes must be compliant with the current legal framework and there is a need for having robust checks and balances. Having an accountability framework based on PMP adds red tape, it does not remove it. To ensure compliance with the PMP there should be fines imposed on organisations. The fines imposed could be determined by the ICO.

Data Protection Officer Requirements

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'? Please explain your choice and provide supporting evidence where possible.

Somewhat agree. The Data Protection Act 2018 introduces a duty to appoint a data protection officer (DPO) for a public authority or for organisations that carry out certain types of processing activities. This could indeed be a costly and slightly burdensome requirement for some organisations. Nevertheless, having an independent DPO with expertise in data protection is crucial for data protection compliance. Under the UK GDPR, a data protection officer can also be an existing employee. This makes it relatively easy and less costly for organisations to appoint a DPO.

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. As noted by the ICO, the introduction of data protection officers has brought significant experience and benefits for organisations and DPOs undertake important compliance functions in several sectors including finance, health, and safety.[12] Furthermore, the requirement to appoint a dedicated role to ensure compliance is a widely adopted approach in many different sectors such as finance, health, and safety[13]. Hence, removing the existing requirement to designate a data protection officer will significantly reduce data protection compliance and will potentially have an impact on UK's adequacy status. Furthermore, the DPO role represents a universally accepted point of contact for private and organisational counterparts and data subjects, i.e., for data subject access requests.

Q 2.2.6 Please share your views on whether organisations are likely to maintain a similar data protection officer role, if not mandated.

If it is not a mandatory requirement, many organisations are not likely to maintain a similar data protection officer role. This is likely to have a negative impact on compliance. Moreover, we are concerned that this may harm UK's data protection

[12] Information Commissioner's Office " Response to DCMS consultation " Data: a new direction" p.18 <https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf>, accessed 29 October 2021.
[13] Ibid.

regime and may have repercussions on UK's adequacy status. If the UK loses its data adequacy status, there will be significant costs on organisations that may offset any cost savings by not appointing a data protection officer. Compliance under relevant legislation cannot be managed without equivalent functions so there is little to be gained by allowing it to be called something else, or to allow it to be split up between several individuals.

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. As noted by the European Data Protection Supervisor, data protection impact assessments (DPIAs) provide a structured way of thinking about the risks to data subjects and how to mitigate them[14]. In other words, DPIAs are powerful tools that enable organisations to identify risks and take appropriate steps to manage and mitigate these risks at the onset of collecting personal data before a risk occurs.

Q.2.2.8. To what extent do you agree with the proposal to remove the requirement for organisations to undertake data protection impact assessments?

Strongly disagree. Data protection impact assessments (DPIOs) ensure that personal data is protected effectively, and enforcement action is taken if necessary. Removing this requirement may have an adverse impact on the protection of personal data and the rights of data subjects. Whilst there may be a need for some flexibility as to how these assessments are conducted, removing the requirement as a whole is neither desirable nor sustainable for an adequate data protection regime.

Prior consultation requirements

Q. 2.2.9 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.

There could be several reasons for this. First, there may not be many organisations that have identified a high risk that cannot be mitigated. Second, some organisations may not fully understand what is meant by high risk and may not consult with the ICO despite the need to do so.

Q.2.2.10. To what extent do you agree with the following statement: 'Organisations are likely to approach the ICO before commencing high risk processing activities on a voluntary basis if

[14] European Data Protection Supervisor Data Protection Impact Assessment< https://edps.europa.eu/data-protection-impact-assessment-dpia_en> accessed October 29, 2021.

this is taken into account as a mitigating factor during any future investigation or enforcement action'?

Somewhat agree. If this is taken as a mitigating factor during any investigation or enforcement action, it might be a sensible way to incentivise organisations to approach the ICO for advice. However, there may be other ways to incentivise organisations to approach ICO before commencing high risk processing activities. For instance, ICO could prepare a case study showcasing the financial and non-financial benefits of consulting with the ICO such as increased trust from data subjects which may lead to financial benefits. Also, there could be other financial incentives offered for consulting with the ICO for high risk processing activities such as public R& D grant funding.

Record-Keeping Requirements

Q.2.2.11. 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. As noted by the ICO, keeping good records is a crucial element of good privacy management and to ensure high standards of privacy[15]. Furthermore, this helps organisations to effectively respond to data subject requirements such as the right to access or data portability and ensure that these requests are not overlooked. Hence, record-keeping requirements should not be removed. However, there could be ways to reduce the burden on organisations by simplifying the record-keeping process particularly for the small and medium-sized organisations which do not undertake high-risk processing. Instead of removing the requirement for record-keeping, the process could be simplified by issuing straightforward guidance to organisations as suggested by the ICO[16].

Q.2.2.12. To what extent do you agree with the proposal to reduce burdens on organisations by adjusting the threshold for notifying personal data breaches to the ICO under Article 33? Please explain your answer, and provide supporting evidence where possible and in particular: ○ Would the adjustment provide a clear structure on when to report a breach? ○ Would the adjustment reduce burdens on organisations? ○ What impact would adjusting the threshold for breach reporting under Article 33 have on the rights and freedoms of data subjects?

Somewhat disagree. Adjusting the threshold for notifying personal data breaches could potentially help reduce burdens on organisations. On the other hand, altering the threshold for breach reporting may harm the rights and freedoms of data subjects. In this respect, as suggested by the ICO the appropriate threshold for notification must be seriously considered and a comprehensive assessment of risk needs to be undertaken as some harm may cause little individual harm to individuals but may be

[15] Information Commissioner's Office " Response to DCMS consultation " Data: a new direction" par. 70 p. 45 <https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf > accessed 29 October 2021.
[16] Information Commissioner's Office " Response to DCMS consultation " Data: a new direction" par. 71, p. 46 <https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf > accessed 29 October 2021.

significantly harmful to society[17]. It must be noted that many countries with developed privacy regimes such as Singapore have introduced compulsory data breach notifications. Hence notifying personal data breaches should be the norm and adjusting the reporting threshold should not undermine the requirement.

Voluntary undertakings process

Q.2.2.13. 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.

Somewhat agree. The proposal to introduce a voluntary undertakings process can be indeed beneficial. However, as observed in other areas of law such as under the Competition Act 1998, where the Competition and Markets Authority retains discretion on commitment decisions, the ICO should also retain the authority to monitor that compliance has been achieved by a remedial action plan. If the ICO is not satisfied with the implementation, it should be allowed to intervene and make changes to the proposed remedial action plan as well as impose fines to an organisation for serious data breaches.

Further questions

Q.2.2.14. 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.

If Article 33 is amended, there could also be a need to amend Article 34 which concerns the communication of personal data breaches to the data subjects. In particular, the exemptions under Article 33(4) which enables organisations not to communicate data breaches to data subjects may be extended. However, as noted above making these changes could seriously undermine the rights of data subjects and require careful consideration.

Q.2.2.15. 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.

If any requirements such as record keeping are removed from the UK GDPR, there should be additional safeguards that need to be put in place to mitigate any possible risks. This would require the ICO's remit to be extended so that it can conduct regular audits to ensure that organisations have an efficient privacy management programme. Furthermore, if a privacy management programme is to be adopted, there could be a need for developing a well-functioning internal and external audit process. Such an audit process would, of course, lead to additional requirements i.e., demonstrating

[17] Information Commissioner's Office " Response to DCMS consultation " Data: a new direction" par. 54 p. 41 <https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf > accessed 29 October 2021.

adequate record-keeping and adequate processes on top of current legislation so this would add more complexity and red tape.

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? 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.

Somewhat disagree. Some elements of Article 30 may be considered duplicative. However, it must be noted that Article 30 is an important safeguard to protect the rights of data subjects. We are concerned that the removal of this requirement may have an adverse impact on compliance and adversely affect the rights of data subjects. Furthermore, this would threaten the adequacy decisions of the UK and may place a significant burden and risk for organisations that would need to interpret complex legislation.

Q.2.2.17. 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 agree. The proposal to amend the breach reporting requirement could be implemented without the implementation of the privacy management programme. However, we believe that the breach reporting requirement is an essential element of accountability. Hence, if this proposal is implemented there need to be additional safeguards in place to protect data subjects whose personal data is compromised.

Q.2.2.18. 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. As noted earlier, appointing a data protection officer could create costs for a small public authority, which could indeed be problematic. However, in a democratic society, public authorities should adhere to the same standards as private organisations. In many sectors, such as procurement, it is common to require the same standards from public authorities as private organisations. The DPO role is not necessarily a full-time job – it's fundamentally about ensuring accountability by naming a responsible person. Instead of removing the requirement, there could be some flexibility around the appointment of DPOs.

Q.2.2.19. If you agree, please provide your view which of the two options presented at paragraph 184d(V) would best tackle the problem.

We do not agree with the above.

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?

There could be some amendments to Art. 77 to 84 which concerns remedies and liabilities. In terms of penalties introduced, small and medium-sized enterprises could be exempted from penalties depending on the severity of the infringement. There could also be a reduction in penalties if the organisation cooperates with ICO during the investigation process. Also, if an organisation has not infringed on the GDPR previously there could be some leeway. This could indeed incentivise organisations to report data breaches.

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

There is some evidence that organisations can find responding to data subject access requests a time-consuming and/or costly process. This is not to, however, a stick with which to beat the right of access to personal data. The right of access is a critical right upon which the effective use of other rights (e.g. the right to erasure etc.) is hugely dependent. The possible inference that high costs/time demands are reflective of a flaw in the construction of the right of access itself, or that it should somehow be restricted or further qualified, must be resisted. Difficulties in complying with a legal obligation are not, in themselves, reasons for doing away or weakening said obligation if the rationale behind it, and its intended effect, are worthy of pursuit. As alluded to above, the right of access protects a number of vital interests of the data subject, and data controllers should not be able to absolve themselves of their responsibilities simply because responding to access requests can be inconvenient to them. If an organisation deals with, stores, or relies upon the processing of the personal data of others in order to generate revenue, costs (within reason) accrued by responding to subject access requests should be seen as a constituent and built-in cost of operating in their chosen way. An organisation dealing with toxic or dangerous substances would never be allowed to exempt themselves from environmental regulations to which they are subject on the basis of it being inconvenient to comply with the law, and by the same token neither should an organisation dealing with personal data. Difficulty in complying with the law is not, and has never been, an excuse or justification for non-compliance.

That said, there are some issues inherent in the right of access that would perhaps benefit from address. Vexatious requests can certainly be an issue for some data controllers. I am aware personally, for instance, of subject access requests that have been made for the sole purpose of annoying the head of a department, and of individuals “weaponizing” subject access requests (i.e. bombarding a data controller with multiple requests) purely for the sake of causing as much disruption as possible. Behaviours of this sort are clearly not within the spirit of the law, and data controllers should not be forced to dedicate resources to responding to access requests that are made in bad faith. The difficulty, however, is in determining how, when and in which circumstances a request is either vexatious and or made in bad faith, and indeed who it is who makes this determination.

One major issue relating to subject access requests, and data controller responses to them, will often be a lack of expertise. Though large organisations will frequently have their own data protection officer and/or in-house legal team, smaller organisations will not possess staff with any degree of data protection expertise (though often even small businesses designate a

member of staff as being nominally responsible for data protection matters). Subject access requests are currently viewed by staff of many smaller organisations as a vague and confusing process. Such staff often operate on a "will this do?" basis, with information provided to data subjects often being dictated by the internal rules of an office, or what a more senior member of staff (without any detailed knowledge of data protection law) may (possibly erroneously) believe is the law. This is a plainly unsatisfactory situation, but one that could be improved drastically by even the most basic of data protection training courses.

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'?

○ **Somewhat disagree**

The threshold is not too high. As data subjects may have very pressing and important reasons for making data subject access requests, it is right that data controllers should only be able to refuse such requests in very limited circumstances. However, the meaning of "manifestly unfounded" is vague and would benefit from clarification.

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?

○ **Somewhat disagree**

This is a problematic suggestion. It is all very well and good suggesting that data controllers should be able to refuse "vexatious" or "manifestly unfounded" subject access requests, but in practice these terms will mean different things to different people. What might be vexatious in the eyes of a data controller may be anything but in the eyes of a data subject. If determinations as to vexatiousness are to be made by data controllers alone, this potentially allows for them to ride roughshod over the valid interests and concerns of data subjects in how their personal data are handled and used by other parties. Why should a data controller be given the power to determine that their interests in not responding to a subject access request are in any way deserving of priority over those of a data subject seeking their personal data?

The test used under the Freedom of Information Act 2000 states that requests can be denied when they are "likely to cause a disproportionate or unjustifiable level of distress, disruption or irritation." This test would not easily translate into a data protection context. In respect of a subject access request for personal data, for instance, how on earth would a data controller be able to effectively and consistently determine whether responding to (or refusing to respond to) such a request would lead to a "disproportionate level of distress". This calculation could only be made with a full knowledge and appreciation of the data subject's personal circumstances and the reason behind their request, which they would not have (and the data subject should not be compelled to provide).

In any event, calculating whether a subject access request is "vexatious" according to the above standard would, because of amount of different factors that would need to be considered, would be a hugely resource-intensive and time-consuming task, so if the aim is to

reduce burdens on data controllers it is doubtful that this idea would achieve the desired objective.

Placing cost limits on data subject access requests would also be potentially problematic. If this suggestion were pursued, adequate safeguards would have to be established to ensure that perfectly valid data subject access requests were not defeated by costs alone.

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

The idea of allowing data controllers to impose costs for responding to subject access requests is problematic, and raises questions as to the conceptualisation of data protection rights generally. Data protection rights exist as a means of ensuring individuals fundamental human rights (i.e. as per the ECHR) are afforded adequate protection in the context of harms that could potentially arise from the processing of their personal data. Ergo, data protection rights are an extension of human rights. A necessary implication of allowing data controllers to charge fees for responding to data subject access requests, therefore, is that requiring individuals to pay money in order to have their fundamental rights enforced is an acceptable practice, or at least that the application and enforcement of human rights can be measured in monetary terms. Both implications are troubling. In any event, if nominal fees were introduced, it would be important to ensure adequate safeguards were established, so to ensure that perfectly valid data subject access requests (potentially made for very serious reasons, e.g. to investigate bullying in the workplace) were not made prohibitively expensive for those who were financially disadvantaged.

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

○ **Yes**

If organisations' staff responsible for dealing with data subject access requests received better training, or even basic training in matters pertaining to data protection, it is likely that costs associated with responding to data subject access requests would be reduced (see answer to question 2.3.1). The government should pursue initiatives which incentivise organisations to send their staff on basic training courses pertaining to data protection, and specifically those dealing with how to appropriately respond to data subject access requests.

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'?

These should be strictly defined for aggregate and anonymised data processing that does not include tracking of specific, identifiable individuals. They should only include first-party cookies. The exception should be narrowly defined to avoid misuse and interpretation by data controllers that would include other, unintended, and often harmful purposes.

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?

○ **Strongly disagree**

As noted above, this should be a narrow exception and not a broad removal of consent requirement that could be widened to include 'similar technologies' used to track individuals, by cookies, device fingerprinting or other devices developed by data controllers. This is in line with the E-Privacy Regulation Proposal and views expressed by the EDPB.

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.

○ **Somewhat disagree**

Consent exemptions should be narrow and limited to what is strictly necessary. By defining the circumstances broadly and/or vaguely, these could be interpreted widely by data controllers, resulting in a function and purpose creep, and consequently, different types of privacy violations (tracking, manipulations, nudging etc.). Relying on legitimate interest can open the door for unwanted practices, tracking and manipulating personal data, which we have seen many of in the past years. The purpose of detecting technical faults/safety is an example of a good exemption, again defined narrowly and to what is strictly necessary. In terms of enhanced functionalities, these open the door to broad interpretations by data controllers, which we should avoid in any case when it comes to tracking individuals online.

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**

The UK GDPR principles on lawfulness, fairness and transparency and consent as a lawful basis would still need to apply, and this should not be compromised. As establishes by the A29 Working Party,[18] cookies are personal data in most cases, and UK GDPR bases for processing must apply. Legitimate interest may be an appropriate basis for a limited number of first-party cookies, where risks to individual rights and freedoms are low, and these are mostly analytics and cookies used for safety purposes narrowly defined. For tracking and third-party cookies, in particular, consent must be retained as a lawful basis.

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?

Potentially yes, but these would need to be reviewed/approved by the ICO and in accordance with exemptions clearly set out in the law.

[18] Opinion 04/2012 on Cookie Consent Exemption, WP 194 (07.06.2012).

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?

Key benefits to the protection of privacy arise if these are privacy by default settings. User preferences to the contrary should be expressed clearly by changing the privacy-protective settings. Websites and advertisers should be clear as to what these are. This way, users could be more in control. Risks relate to user awareness and interaction with such settings, given media literacy issues and consent fatigue, which have been widely evidenced in the recent literature.

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

Browser technology has the potential to reduce the volume of cookie banners in the future to a very good extent if set to privacy by default position.

Q2.4.9. To what extent do you agree that the soft opt-in should be extended to non-commercial organisations? See paragraph 208 for description of the soft opt-in.
○ **Somewhat agree**

This could benefit charities and other similar organisations, as noted in para 208 of the consultation paper. However, these organisations need to be clearly defined to exclude any organisations that engage with en masse tracking of individuals behaviours.

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.

This is a good suggestion in our view.

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.

This is a good suggestion as it increases transparency. Organisations should be required to report these in a meaningful way. Perhaps parameters could be set by the ICO,

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?

Spam of different sorts has historically been tackled best by technology and services providers. Measures such as filtering, blocking, blacklisting etc. are best placed to handle these problematic communications effectively.

Q2.4.13. Do you see a case for legislative measures to combat nuisance calls and text messages?
○ No

As noted above, technology and service provider work has proven to be a better, more effective way to address these problems ever since spam in the early days of the Internet.[19]

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

As above, numerous benefits, e.g. less nuisance, efficiency. Risks: blocking other, legitimate calls, technology glitches.

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.

This is a reasonable suggestion and ties in with what we noted above.

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)?
○ Strongly agree

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 them to carry out audits of the organisation's processing activities?
○ **Strongly agree**

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?

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

They should absolutely be covered. There is no good reason for why communications sent by registered parties for political campaigning purposes should enjoy any sort of special exemption from the PECR rules on direct marketing.

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?

[19] See Lilian Edwards, 'Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling' in L Edwards, ed, *Law, Policy and the Internet,* Hart, 2019.

○ **Somewhat agree**

Yes, this is not an unreasonable idea. In situations where individuals had, for instance, attended a conference or other event for a specific political party, it seems unlikely that they would envisage their personal data being processed for the purposes of sending follow-up communications and similar would be in any way unreasonable and/or unexpected. So long as individuals' right to opt out, and their ability to exercise other data protection rights in conjunction with such uses of their personal data, were safeguarded, there is nothing prima facie objectionable to this proposal.

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? See paragraph 208 for description of the soft opt-in

○ **Neither agree nor disagree**

This proposal would need to be approached with a degree of care. Though there is nothing necessarily prima facie wrong with this idea, registration with the Electoral Commission should not be taken as a sign that a third party is automatically trustworthy or reputable, or that it should be assumed to be a responsible custodian of personal data. Some third party campaign groups might have, or are perhaps likely to have, extreme views (e.g. views relating to sexuality, gender roles, race etc.). Individuals are likely to have entirely legitimate interests in their personal data not entering the possession of such parties non-consensually. Accordingly, whether (and, if so, when) the soft-opt in should be extended to organisations and bodies of this sort will have to be carefully thought out, and appropriate safeguards will have to be put in place to prevent abuses.

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?

○ **Somewhat disagree**

This is a vague and ambiguous question. The term "democratic engagement" allows for a broad spectrum of interpretation, so it is not at all clear to what sort of activities this question is intended to apply. Assuming "democratic engagement" does not encompass any particularly unusual activities, however, there appears to be no obvious reason as to why any of the lawful grounds of Art 6 of the UK GDPR would act as an overly restrictive or unfair impediment to their accomplishment. Even if Art 6 does represent such an impediment, there does not seem any reason to suggest such an impediment would be unjust, nor does there seem to be any compelling reason as to why "democratic engagement" activities should be in any way exempt from, or enjoy a "light touch" application of, data protection rules.

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**

As suggested above, it is not entirely clear to what the term “democratic engagement” applies. If, however, we are to assume the term encompasses activities such as political fundraising, political surveys, opinion polling and similar, paragraphs 22 and 23 do not represent an unjust impediment to their accomplishment. Paragraphs 22 and 23 set out clear and sensible rules regarding when personal data can be processed for these purposes, and crucially, when they cannot. There is absolutely no need, nor is there any justification, for any relaxing of the rules and provisions set out in paragraphs 22 and 23.

Chapter 3

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?*
○ Strongly disagree

The Consultation document raises the question: how much leeway does the UK have when designing its data protection adequacy decision framework? The government is proposing to afford itself a great degree of freedom and do so on the basis that in the past jurisdictions such as Israel have been deemed adequate “while pursuing independent and varied approaches to data protection, reflecting their unique national circumstances, cultures and heritages” (para 15).
On this basis, the government is proposing that adequacy decisions be "risk-based and focused on outcomes", rather than a "largely textual comparison of another country's legislation" considering "academic or immaterial" risks. However, it is not clear whether the UK intends to adopt a narrow approach to risk-based adequacy decisions similar that which infuses GDPR adequacy assessments or whether the intention is to develop a broader approach akin to that previously found in Japanese and currently underpinning Australian law. This response cautions against adopting a broad, risk-burden approach and focusing only on material risks for the reasons set out below.
The broader approach (also known as the risk-burden balance model) appears at first glance to be lighter touch, responsive, and proportionate because it requires data enforcement authorities to target risk rather than all data processing activities, and specifically exempts entities that are designated as presenting no danger for individuals (e.g., small entities, or holders of limited amounts of personal data for short time periods) from data protection regulation requirements.
In Japan, entities that held personal data on less than 5000 individuals for less than 6 months were exempt from the data protection obligations.[20] However, this exemption was removed to reflect modern business practices and changes in individual’s privacy cybersecurity and privacy expectations, with the effect that all private business operators are now considered "Handling Operators" covered by the APPI, thereby widening the scope of application of the legislation.

[20] The Act on the Protection of Personal Information, (Act No. 57, 30th May 2003), (the 'APPI'). Article 2 of the Order for Enforcement of the Act on the Protection of Personal Information (Cabinet Order 506, 2003, enacted on 10 December 2003. This exemption was abolished when the APPI was revised in 2017.)

In Australia, subject to a number of exceptions, the Privacy Act 19888 does not currently apply to businesses with an annual turnover of less than $3 million.[21] However, a review (currently ongoing) of the Privacy Act has sought feedback on whether the exemption strikes the right balance between avoiding imposing unnecessary regulation on small businesses and protecting the privacy rights of individuals. Submissions have noted that technological advances (e.g. using computers for data processing, and the web for online business operations), in the 20 years since the small business exemption was introduced have changed the way that small businesses operate and increased the privacy risk they pose.[22] For example, 'even the simplest website could collect information including IP Address, timestamps of visits and which web browser and operating system a visitor used,'[23] and businesses actively engaged in online sales are likely to collect far more information.[24] Small businesses also have access to tools such as 'Facebook pixel' which 'allow businesses to track customers across devices and show targeted advertising to people who have already visited the business' website, or to people who are similar to those already interacting with the website.'[25] Accordingly, many submissions have called for a removal of the small business exemption on the basis that annual turnover is not an accurate proxy for potential impact on privacy.[26] Accordingly, an individual's privacy should not depend on the size or profitability of the entity they are dealing with.[27] Submitters also noted that the exemption does not reflect consumer expectations or the seriousness of a potential breach.[28] An organisation that holds information as basic as name and address could potentially use or disclosure it in circumstances which could cause harm to an individual.[29]

The Japanese and Australian experiences confirm that a broad approach to risk-based adequacy assessments can lead to undesirable outcomes. If exempted based on size (e.g., number of employees, volume of data processed or revenue generated), a small, bad actor could cause a lot of harm, which would be undesirable.

In my view, a narrower interpretation of risk is reflected in the UK GDPR, which retains the approach adopted by the GDPR, or should do if the UK intends to remain compliant with the letter and spirit of the GDPR, to ensure retention and renewal of the EU-UK adequacy decision. The narrow interpretation views risk 'as a yardstick to tailor data controllers' obligations.'[30] For example, the rationale underpinning categorisation is of data as 'special

---

[21] 6D Privacy Act 1988

[22] Submissions to the Issues Paper: New South Wales Information and Privacy Commission, 2; Salinger Privacy, 10; elevenM, 2; Calabash Solutions, 5; Centre for Media Transition, University of Technology Sydney, 10; Consumer Policy Research Centre, 4; Australian Communications Consumer Action Network, 9; Institute for Cyber Investigations and Forensics, University of the Sunshine Coast, 2; Office of the Victorian Information Commissioner, 4; Minderoo Tech and Policy Lab, University of Western Australia Law School, 29; Association for Data-driven Marketing and Advertising, 13; Superchoice, 2; Queensland Law Society, 2; OAIC, 59; Gadens, 1; Australian Privacy Foundation, 14; Australian Information Security Association, 10; CrowdStrike, 3; Data Republic, 5; Privacy108, 4; Queensland Council for Civil Liberties,4; Shogun Cybersecurity, 2.

[23] Submission to the Issues Paper: Minderoo Tech and Policy Lab, University of Western Australia Law School, 29.

[24] Ibid.

[25] Ibid.

[26] Submissions to the Issues Paper: Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 12; Centre for Cyber Security Research and Innovation, 11; Department of Health Western Australia, 3; Australian Information Security Association, 10; CrowdStrike, 3; CSIRO, 5; Data Republic, 5; Shaun Chung and Rohan Shukla, 12.

[27] Submissions to the Issues Paper: Calabash Solutions, 5; Institute for Cyber Investigations and Forensics, University of the Sunshine Coast, 2; Electronic Frontiers Australia, 4; Dr Kate Mathews Hunt, 6; Financial Rights Legal Centre, Consumer Action Law Centre and Financial Counselling Australia (joint submission), 12; Dr Chris Culnane and Associate Professor Ben Rubinstein, 19; Google, 4; Centre for Cyber Security Research and Innovation, 11; New South Wales Council for Civil Liberties, 5.

[28] Submissions to the Issues Paper: Office of the Victorian Information Commissioner, 4; Gadens, 1; Dr Kate Mathews Hunt, 6; New South Wales Council for Civil Liberties, 5; Financial Planning Association of Australia, 2; Professor Kimberlee Weatherill, 4; CAIDE and MLS, 4; Queensland Council for Civil Liberties,4; Financial Services Council, 10.

[29] Submission to the Issues Paper: Queensland Council for Civil Liberties,4;

[30] Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions "A

category/sensitive' or 'ordinary' is that although the harm that can be caused to privacy normally depends on the context in which data are processed rather than on the content of the data as such certain special categories of data do by their nature pose a threat to privacy.[31] In essence, there is an *a priori* presumption of risk in relation to special category data independent of the actual processing context such that the legislator relies on the precautionary principle as to its processing in the form of more stringent obligations e.g., explicit consent apply to reflect the higher processing risk.

Likewise, at the heart of the UK GDPR is a general interest in conferring control over personal data to individuals even in the absence of tangible or intangible harm. Therefore, although making data controllers responsible only for 'material' privacy harms caused by the data processing and allowing them to choose the means to assess and mitigate the risks would align with the APEC Privacy Framework and its primary principle of prevent harm to individuals, it would be problematic because it would conflict with a core tenet of the UK GDPR.

In summary, the UK's future approach to adequacy decisions should comprise a mix of textual comparison of another country's legislation to ensure that core data protection principles and data subjects rights are guaranteed by data controllers irrespective of the level of risk to data subjects or level of harm posed, and a narrow interpretation of risk should be adopted in respect of adequacy decisions to ensure scalable and proportionate compliance e.g., more stringent obligations in respect of special category data processing. And, as the narrow interpretation of risk would ensure continued alignment with the GDPR, would be welcomed by businesses with UK and EEA operations that are currently based in the UK and seeking to minimise their compliance burdens.

Paradoxically adopting a broader approach to risk regulation that prima facie focuses only on 'serious' harms' or 'material risks' would prove counter-productive in terms of data flows from the EU/EEA bloc, potentially imperilling the EU-UK adequacy decision (or its renewal), add to the compliance burden of businesses established in the UK for the purpose of trading with UK and EEA countries, and therefore potentially reduce the UK's attractiveness as a base for international data flows. Indeed, as Antony Walker of TechUK has observed

> "If you are running [a] global operation, you will want to have consistent processes across your businesses. What we are seeing is that global firms based outside of the EU are taking the GDPR as the norm for their business and are building their processes around it, so, for very large companies, there is no desire to diverge from the GDPR—the opposite, because they worry about falling between the gaps."[32]

In short, the opportunity to diverge may prove illusory. That is, divergence is theoretically possible but may prove difficult to operationalise given that the UK needs data from EEA countries and other third countries will also continue to comply with the GDPR to ensure

---

comprehensive approach on personal data protection in the European Union", 14.1.2011, ("The higher the risks, the higher the need to implement concrete measures that protect information at a practical level and deliver effective protection", 21. EDPS claims that data protection law should be scalable, excluding the requirements of privacy by design, data protection officers and privacy impact assessments which should remain mandatory, 22-23).

[31] Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Amended Proposal"), COM (92) 422 final - SYN 287, 15 October 1992.

[32] House of Lords, European Union Committee, 'Brexit: the EU data protection package,' 3rd Report of Session 2017-19, 18 July 2017, HL Paper 7, para 128.

continued market access. So divergent UK law could simply add friction and could prove an unwelcome business cost.[33]

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*?

○ Somewhat agree

○

The Government is proposing to extend its ability to make adequacy assessments to include groups of countries, regions, and multilateral frameworks (paragraph 248), no doubt because efficiencies could be gained from assessing the laws applicants with similar provisions. Whilst the government might want to prioritise 'data partnerships' with countries it is negotiating trade deals with, e.g., the US, this approach could lead to it getting bogged down for years in negotiations with a country with widely divergent standards or succumbing to pressure to lower its own standards to facilitate trade, which could have negative consequences e.g., jeopardising the EU-UK adequacy decision. Accordingly, it is suggested that the government should instead prioritise the assessment of countries that have acceded to Convention 108+ because the modernised Convention contains many similar provisions to those in the UK GDPR. Whilst this would speed up the assessment process it is important to note that Convention 108+ does not include enforcement provisions found in the UK GDPR so it would not be a mere 'rubber stamping' exercise.[34]

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*?

○ Strongly disagree

.

The Government also proposes removing the need for periodic review of adequacy decisions, which currently must take place every four years (paragraph 250) and replacing it with an 'ongoing monitoring' requirement. However, the Government has not specified how it intends to ensure 'ongoing monitoring'. Building a degree of flexibility into the periodic review period would be more appropriate than removing the requirement to review adequacy regulations every four years altogether or introducing a vague ongoing monitoring requirement. For example, the government could have a mechanism for extending the review period beyond four years if it was notified by a third country that the review period would overlap with a period in which the third country intends to implement legislative or procedural changes. In such circumstances it could be appropriate to delay the periodic review until the changes have taken effect. Having said that, any extension period should be for a specified period e.g., 18-24 months. And, if the third country fails to complete the legislative reform programme within the specified period, then the UK government should have a mechanism for triggering the postponed review or deciding to halt transfers to the country until compliance with the UK GDPR can be confirmed. The advantage of this approach is that it would allow a schedule of work to be planned, resources e.g., staff and other resources to be allocated, and avoids accidental drift and non-compliance with the UK GDPR over time.

[33] Mc Cullagh, Karen, **'**Post-Brexit Data Protection in the UK - Leaving the EU but not EU data protection law behind*,' in Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics,* Van Brakel, R., De Hert, P. & González Fuster, G. (eds.). (Edward Elgar Publishing forthcoming).

[34] Greenleaf, Graham, 'Modernised' Data Protection Convention 108 and the GDPR (July 20, 2018). (2018) 154 Privacy Laws & Business International Report 22-3, UNSW Law Research Paper No. 19-3, <https://ssrn.com/abstract=3279984>

Additionally, the government should consider whether continued close alignment with the GDPR would allow it to develop a working relationship with the EU such that a mechanism/procedure could be developed to allow the UK to 'rubber stamp' any adequacy decision renewals by the European Commission. That is, if the UK GDPR and GDPR remain essentially equivalent, then as and when the European Commission completes a periodic review of adequacy, the Secretary of State could have a mechanism that accepts renewal of a GDPR adequacy decision as a proxy for periodic review under the UK GDPR, thereby reducing the UK's assessment burden by avoid unnecessary duplication of assessments.

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*?
○ Strongly agree

The Government is proposing to amend the UK GDPR to make it clear that both judicial (e.g., provided for by a court of law or tribunal) and administrative (e.g., provided for by a regulator or ombudsperson) redress are acceptable so long as the redress is effective (paragraph 254). Both forms of redress can be equally effective, provided they are available in a timely manner, cost-effective, and any remedies awarded are legally binding.

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*?
○ Strongly disagree

The government Is proposing to permit "repetitive use of derogations" (270). Repetitive use of derogations could leave the UK in breach of the spirit of the EU-UK GDPR adequacy requirements, because they should only be used in exceptional circumstances. Accordingly, if the UK does proceed with this proposal, it should require a data exporter to only avail of the derogation on a repetitive basis in very limited circumstances and require the data controller document the necessity and proportionality arguments regarding reliance on the derogation and to document the safeguards they have put in place.

Chapter 4

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'?

○ **Strongly disagree**

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

Public sector organisations should not be authorised to share personal data for the sake of the advancement of private companies (many of whom will have interests that are contrary to those of data subjects to whom such data relate). Giving public sector organisations legal authority to disclose personal data to private companies for the sake of those companies' advancement would effectively introduce a major carve out/exemption to a wide range of data protection rules and principles, and in so doing would seriously diminish and limit the application of data protection law, and concurrently weaken the level of data protection enjoyed by individuals.

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?

○ **Neither agree nor disagree**

The term "substantial public interest" is indeed somewhat vague. Clarification of this term, and the role it plays in legitimising the processing of special category data, would likely be welcome. However, the devil will be in the details (i.e. how and in what way the term is clarified). The proposal at present does not clearly explain what any clarification of this term would consist of/look like. Further detail regarding this proposal will be necessary in order to provide greater feedback in relation to whether this is a good or bad idea. However, as above, in principle, there is nothing objectionable with attempting to add greater certainty to this part of the legislation.

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

If this proposal were to be pursued it would be important that adequate safeguards were built into whatever clarification was adopted to ensure it was not abused. Greater clarity of the term "substantial public interest" should not equate to making it "easier" for data controllers to process health. The purpose of the clarification should exclusively be to help data controllers to determine when they were able to process personal data on this basis, not broaden their opportunities to process personal data on this basis.

Whatever clarification of the term "substantial public interest" is eventually settled on, it will be important for this clarification to be accompanied by explanatory notes/text that make it clear that this part of the legislation can only be invoked in exceptional circumstances, and that data controllers should be required to demonstrate why whatever public interest the processing of health data is necessary to protect is "substantial".

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

○ **Somewhat disagree**

Public authority usage of algorithmic/automated decision-making should absolutely be subject to rigorous transparency requirements. This is absolutely vital for the purposes of democratic, political, and legal accountability. That said, the extent to which such requirements will greatly enhance widespread public trust in public uses of personal data is perhaps doubtful.

The algorithms that are likely to be used to underpin any public sector automated decision-making are likely to be highly complex and sophisticated. Regardless of whatever transparency obligations are put in place, it is unlikely that they will be explainable in plain

language that would be understandable to all sections of the general public. Full appreciation of the usage of algorithms in any context would likely require a degree of expertise that the average person simply does not possess. To this end, it is probably unlikely that greater transparency would engender a widespread increase in public trust.

Moreover, there is a chance that public sector algorithms may fall foul of the so-called "black box problem", whereby they will begin to behave/make decisions in ways that are insusceptible to human cognition and comprehension.

More broadly, as has been pointed out elsewhere, transparency obligations (i.e. legal requirements which require explanations to be provided to individuals) frequently tend to be vague and unclear in relation to whom and to what they apply (Edwards 2017, Veale and Edwards 2018).

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

At the very least, transparency requirements should compel public sector organisations to provide explanations in relation to what personal data are subject to algorithmic/automated decision-making, which/what algorithmic techniques and technologies were being applied to the personal data, how these algorithms operated, what the purposes of the use of algorithms were, what safeguards are in place to prevent bias/discrimination/other harmful consequences, and how decisions made by algorithms can be challenged and/or reviewed by a natural person.

As above, however, for the reasons given in relation to Q.4.4.1, transparency obligations are unlikely to achieve much alone. A greater suite of legal rules relating to public sector algorithm use would likely go to greater lengths to increasing public trust and confidence in this area (e.g. stronger legal rules, restrictions and controls on public sector algorithm usage, greater access to judicial review as a means of challenging erroneous and/or unfair/harmful algorithmic decisions).

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

Exemptions for transparency reporting requirements on the use of algorithms in decision-making by public authorities and government bodies/contractors should be strictly limited and construed very narrowly. Automated/algorithmic decision-making is increasingly used as the basis for decisions about individuals that can literally be life-changing, and so it is vital for individuals to have effective means through which they can challenge such decisions in the event of suspected impropriety or similar.

The ability for individuals to scrutinise public sector decision-making is absolutely critical to ensuring effective political and democratic accountability. By the same token, the ability of individuals to ascertain, who is processing their personal data, in what circumstances, and for what purposes, is a prerequisite for them effectively exercising their other data protection

rights (e.g. the right of access, right to erasure etc.). To this end, there is a clear reason for why transparency reporting obligations must remain in place for the majority of algorithmic decision-making undertaken by public sector organisations. The consequences of such obligations being removed or watered-down would likely be extremely harmful.

There may on occasions be reasons to limit transparency obligations in the above regard (e.g. in situations where revealing information about the decision-making process may represent a significant risk to national security or to public health), but as above, such exemptions should be limited to truly exceptional circumstances and construed very narrowly so that they do not become subject to abuse.

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

○ **Neither agree nor disagree**

No comments.

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

○ **Somewhat agree**

Yes, as noted above in response to Q4.3.3 the term "substantial public interest" is vague and would likely benefit from clarification. To this end, it is unclear what the word "substantial" adds to the term "public interest" (i.e. a ground for personal processing under Art.6 UK GDPR), or indeed how "public interest" and "substantial public interest" differ. Some elucidation as to their difference can perhaps be gleaned from case law and other regulatory guidance, but statutory/legislative clarification would likely be desirable. However, as also noted above, whether such clarification would be a development to be welcomed would depend heavily on exactly *how* the term was clarified, and *what* the eventual wording of the clarification was.

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

○ **Somewhat agree**

See above (answers to 4.3.3 and 4.4.5).

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 agree**

It would likely be helpful if a specific "critical public health" (e.g. serious epidemics/pandemics) situation was added to the list of situations mentioned in Schedule 1 that are always deemed to be in the substantial public interest.

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'?

○ **Neither agree nor disagree**

No comments.

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

○ **Neither agree nor disagree**

No comments.

Chapter 5

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?

○ *Neither agree nor disagree*

At present, there is no strategic framework to guide the ICO's work. However, as noted in the Consultation, the ICO currently does identify and publish its strategic priorities in a series of documents (Information Rights Strategic Plan; Technology Strategy; International Strategy). These strategies are set for an appropriate timeframe (for instance, four years in the case of the current Information Rights Strategic Plan). This enables the ICO to strike a suitable balance between clarity and stability, on the one hand, and flexibility in defining its priorities in a changing societal and technological context, on the other.

The evidence that a new statutory framework is required for the objectives and duties of the ICO is unclear. The existing approach can attain the objectives stated in the Consultation document (namely: to "offer greater clarity and stability to the ICO's role and purpose, improve transparency, and strengthen accountability in line with best practice of other regulators"). The case might be made to consolidate the existing Information Rights and Technology strategies, given that technology is now an embedded factor in almost all ICO work. This is the type of change that the current approach enables unimpeded.

Furthermore, it is unclear how this proposal to put the objectives and duties of the ICO in a new statutory framework is reconciled with the broader ambition expressed in the Consultation to "propose more discretion for regulators to achieve their objectives in a flexible way, counterbalanced by increased accountability and scrutiny" (para 316).

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?

○ *_Neither agree nor disagree*

The objective of upholding data rights, monitoring enforcement and providing safeguards to prevent data misuse are core to the ICO. Public trust in personal data processing is also critical to its role, and it should seek to foster trust in data processing. It is not the role of the ICO to encourage data processing or use, however where such processing occurs it should ensure that it is done in a way that enhances trust and confidence.

Q5.2.3. Are there any alternative elements that you propose are included in the ICO's overarching objective?

○ *_Yes*

The primary role of the ICO should be to ensure compliance with the legal framework for personal data processing and to ensure that enforcement action is taken when such compliance is lacking. This, in turn, will lead to increased public confidence in personal data processing.

The independence of the ICO (see further below) from both direct and indirect interference should also be emphasised.

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*

The ICO is required to apply a legislative framework: the Data Protection Act 2018. This legislative framework protects "individuals with regard to the processing of their personal data" (s2). It does this by (i) requiring personal data to be processed lawfully and fairly; (ii) conferring rights on the data subject and (iii) conferring obligations on the Commissioner.

The legislative framework does not explicitly enable economic growth and innovation considerations to be taken into account by the ICO when discharging its functions. While there may be some specific provisions which enable such factors to be taken into account (such as the Article 6(1)(f) legitimate interests legal basis incorporated into the 2018 Act), there are not legal grounds for their incorporation more generally.

Nor is their proposed introduction desirable. Cooperation between the ICO and other regulators such as the CMA whose remit is to ensure the efficient functioning of markets, including the promotion of consumer choice and innovation, is desirable. Nevertheless, requiring the ICO to have regard to economic growth and innovation when discharging its

functions, blurs the boundaries between the competences and functions of these regulators. Moreover, where a direct clash exists between the duties of the ICO to uphold the rights of individuals or to ensure good data governance, on the one hand, and economic growth considerations, on the other, it is unclear how the ICO would or should discharge its duties. This, in turn, would affect legal certainty negatively.

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?
○ *_Neither agree nor disagree.*

More specificity is needed on the idea that the ICO would "have regard to competition" when discharging its functions. The ICO can already take into account the competitive context (eg the extent to which there is a competition on a relevant market) when applying the law. For instance, when ascertaining whether consent can be deemed to be "freely given", the market position of the data controller may be relevant to this assessment. This is distinct from a more proactive role where the ICO would seek to promote competition through its actions. There is a risk with the latter that this encroaches on the regulatory competences of the CMA and detracts from legal certainty (as above).

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 DRCF (CMA, Ofcom and FCA)?
○ *_Somewhat agree*

The principle of inter-agency cooperation is welcome and mirrors developments occurring elsewhere in an effort to ensure more coherent regulatory decision making (for instance, the EU's Digital Clearing House). Whether it is appropriate to impose a *duty* on the ICO to engage in this way, as opposed to merely eliminating the obstacles to such cooperation, depends on what this cooperation entails.

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?
○ *_Don't know*

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?
○ *_Strongly agree*

If the DRCF is to be effective in its mission to ensure effective cooperation between regulatory bodies, then it is necessary for these agencies to discuss the details of the cases they are investigating. In successful examples of inter-agency cooperation (for instance, the European Competition Network), mechanisms and procedures have been introduced to facilitate data sharing while respecting the procedural rights of stakeholders in the investigation. Similar ground rules are required for the DRCF.

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*

Q5.2.10. 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?
○ _*Somewhat disagree*

The ICO is the regulator tasked with upholding fundamental rights and promoting responsible data use. The rights it is required to uphold, in particular the right to respect for private life, have regularly been jeopardised by security initiatives that have subsequently been deemed incompatible with Article 8 ECHR by the ECtHR (for instance, in *S and Marper v UK*). To the extent that the ICO must apply the law in a proportionate way, the obligation to take security factors into account is already present.

It is unclear what the motivation is to render this obligation explicit.

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*

The ICO is an independent regulatory body. Article 15(5) of the Council of Europe's Convention 108 (as modernised) states that:

"The supervisory authorities shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions."

While there is no jurisprudence on this provision from the ECtHR, it is worth highlighting that this text requires *complete* independence. Should the Secretary of State specify, or even influence, the priorities of the ICO, this would constitute an interference with its independence. It is also recalled that EU law views the complete independence of supervisory authorities as an "essential component" of the right to data protection (*Schrems* and subsequent jurisprudence). By politicising the role of the ICO, there is a clear risk that the UK would no longer be deemed adequate by the EU for the purposes of transnational data flows.

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?

○ _*Somewhat disagree*

The ICO already publishes an international strategy, thereby ensuring some transparency. The current strategy is also a structured one. The need for further transparency and structure is therefore unclear.

.

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*

As noted above, the ICO is an independent regulator. By requiring the ICO to take into consideration the government's wider international priorities when conducting its international activities, the government would be explicitly influencing its actions and role for political aims. This would leave the UK in breach of its international legal commitments and in danger of jeopardising its existing data sharing agreement with the EU.

5.3. Governance Model and Leadership - relates to FOI role also.

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?*
○ *_Strongly agree*
○ *_Somewhat agree*
○ *_Neither agree nor disagree*
○ *_Somewhat disagree*
○ *_Strongly disagree*

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

Q5.3.2. To what extent do you agree with the use of the Public Appointment process for the new chair of the ICO?
○ *_Strongly agree*
○ *_Somewhat agree*
○ *_Neither agree nor disagree*
○ *_Somewhat disagree*
○ *_Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.
Q.5.3.3. To what extent do you agree with the use of the Public Appointment process for the non-executive members of the ICO's board?
○ *_Strongly agree*
○ *_Somewhat agree*
○ *_Neither agree nor disagree*
○ *_Somewhat disagree*
○ *_Strongly disagree*

Please explain your answer, and provide supporting evidence where possible.
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 agree*
○ *_Somewhat agree*
○ *_Neither agree nor disagree*
○ *_Somewhat disagree*
○ *_Strongly disagree*

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

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?
○ *_Strongly agree*
○ *_Somewhat agree*
○ *_Neither agree nor disagree*
○ *_Somewhat disagree*
○ *_Strongly disagree*

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

5.4 Accountability and Transparency

The government welcomes views on the following questions:

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?

○ **Strongly agree**

The proposal to strengthen accountability mechanisms and improve transparency to aid external scrutiny of the ICO's performance seems a welcome suggestion. The legality principle is a legal standard in all democratic societies and a key benchmark in public administration. It supports legal assurance, as well as increasing lawfulness in decision making processes. The transparency principle directly affects the liability of public authorities toward the citizens, by allowing these citizens to get access to all information concerning their activity. Lack of accountability and transparency in public administration decreases the rule of law and democratic values. Standardized accountability and transparency requirements enhance public administration. This takes places when the latter regularly publishes information about specific decisions and responds to citizens' requests vis-à-vis their administrative decision-making. The transparency principle also demands that administrative activity be accessible for citizens or open for public review. Thus, transparency and accountability remain key principles for democratic governance[35].

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?

○ **Strongly agree**

The proposal to introduce a requirement for the ICO to develop and publish comprehensive and meaningful KPIs to underpin its annual report appears also appropriate. The transparency principle is a constitutional tenet, which is adopted by the EU institutions as a basic tool for other rules. The concept of transparency has developed from other subjects, varying from social law to legislation on financial issues, as well as recruitment by the EU Institutions. The openness principle was incorporated into EU legislation by the Amsterdam

[35] https://core.ac.uk/download/pdf/229465497.pdf

Treaty, under Article 1 of the Treaty on European Union (TEU)[36]. Furthermore, the UN has portrayed the notions of transparency, accountability and integrity, individually and collectively, as part of the foundational tenets of public administration[37]. Additionally, transparency is deemed to be a key feature of high-quality governance. The EU Ombudsman also made efforts towards legislation on good administration to avoid maladministration. It created the 'Code of Good Administrative Behavior', which encapsulates 27 articles, being basic norms for good administration[38]. Similarly, both the right to good administration and the right of access to documents was incorporated into the EU Charter of Fundamental Rights. On the one hand, Article 41 of the EU Charter enshrines the right to good administration:

'1. Every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions, bodies, offices and agencies of the Union.

2. This right includes: a) The right of every person to be heard, before any individual measure which would affect him or her adversely is taken; b) The right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy; c) The obligation of the administration to give reasons for its decisions.

3. Every person has the right to have the Union make good any damage caused by its institutions or by its servants in the performance of their duties, in accordance with the general principles common to the laws of the Member States.

4. Every person may write to the institutions of the Union in one of the languages of the Constitution and must have an answer in the same language.'

On the other hand, Article 42 of the EU Charter includes the right of access to documents:

'Any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, has a right of access to European Parliament, Council and Commission documents.'

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?

○ **Strongly agree**

Please refer to previous question.

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?

○ **Yes**

[36] Treaty of Amsterdam amending the treaty of European union, the treaties establishing the European communities and certain related acts, oct. 2, 1997, 1997 o.j. (c340).
[37] The UN Charter states, "The paramount consideration in the employment of the (UN) staff … shall be the necessity of securing the highest standards of efficiency, competence and integrity." (Article 101) In addition, many Member States identify integrity, transparency and accountability among core values or founding principles for their public administrations in their constitutions and relevant laws.
[38] https://core.ac.uk/download/pdf/229465497.pdf

In terms of aiding transparency and scrutiny of ICO'S performance, it is the duty of public authorities to publish all information associated with administration activity. Conversely, interested parties should also have equal access to information sources and relevant data. Moreover, public administration's transparency has significant impact on public administration reform, as well as promoting increased effectiveness, efficiency and responsiveness, as key factors of good administration. In this context, public administration's transparency should be supported by the deployment of innovative Information and Communication Technologies. Thus, the computerization and modernization of public administration should be considered fundamental features of government transformation toward a higher degree of open information accessibility, accountability and transparency[39].

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 above.

As noted above, standardized accountability and transparency requirements enhance public administration. This takes places when the latter regularly publishes information about specific decisions and responds to citizens' requests vis-à-vis their administrative decision-making[40].

The government welcomes views on the following questions:

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**

The regulator should be completely independent of any Parliamentary and political influence. The Independent Reviewer of Terrorism Legislation is an illustrative example: in *Big Brother* the ECtHR stressed that the uniqueness of the Reviewer's role lied in 'its complete independence from government'[41]. Moreover, the UN Special Rapporteur's Report on Freedom of Expression stated that any law limiting the right to freedom of expression must be applied by a body that is independent of any political power in a way, which is not arbitrary, including the possibility of remedy and challenge[42]. Additionally, case law from the ECtHR states that, in a field where abuse was highly likely, it was also in principle desirable to entrust supervisory oversight to a judge[43]. Parliamentary scrutiny should be limited to ensuring the regulator fulfils its duties appropriately.

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.

[39] Ibid.
[40] Ibid.
[41] *Big Brother Watch and Others v United Kingdom (*Applications nos. 58170/13, 62322/14 and 24960/15*)* at 160.
[42] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (16 May 2011) at Page 8.
[43] *Klass and others v Germany (*Application no. 5029/71*)* at Para 56 *Big Brother Watch and Others v United Kingdom (*Applications nos. 58170/13, 62322/14 and 24960/15*)* at Para 58.

In view of the previous answer, this question is not directly relevant/applicable.

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?

○ **Somewhat agree**

The European Data Protection Supervisor has noted that the Member States, the European Data Protection Board and the European Commission must support the drawing up of codes of practice considering the specific needs of micro, small and medium-sized enterprises[44]. Similarly, the Article 29 Working Party further observes that compliance with these codes also helps build transparency[45].

The report notes that the government proposes to compel the ICO to carry out and publish impact assessments, as well as undertaking improved consultation, when developing codes of practice, and new or complex guidance. The report explains that this will provide the current procedures with a statutory underpinning. It further elaborates that it is imperative that the ICO's codes of practice and guidance are accessible and allow regulated entities to comply with the law easily and efficiently. Importantly, this would appear to be consistent with human rights instruments such as, the European Convention on Human Rights. It is worth noting that post-Brexit the EU-UK Trade and Cooperation Agreement supports the UK's commitment to remain subject to the ECHR, and the oversight of the ECtHR. In this regard, it should be stressed that, according to the European Court of Human Rights' case-law, for any interference with the right to privacy and freedom of expression to be 'in accordance with the law' under Articles 8 and 10 of the Convention, three conditions must be fulfilled: firstly, it needs to be based in national legislation; secondly, this legislation should be accessible and thirdly, it must satisfy the Strasbourg Court's foreseeability and rule of law principles[46].

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?

○ **Strongly disagree**

As noted above, the European Data Protection Supervisor has noted that the Member States, the European Data Protection Board and the European Commission must support the drawing up of codes of practice considering the specific needs of micro, small and medium-sized enterprises[47]. Similarly, the Article 29 Working Party further observes that

[44] European Data Protection Supervisor (Opinion 3/2018) Opinion on Online Manipulation and Personal Data at Page 20.
[45] Article 29 Working Group Guidelines on Consent under Regulation 2016/679 at pg 19.
[46] *Kennedy v the United Kingdom* App no 26839/05 (2010) 52 EHRR [151]; *Rotaru v Romania* App no 28341/95 (2000) 8 BHRC 449 [52]; *Liberty and others v the United Kingdom* App no 58243/00 (2008) 48 EHRR 1 [59]; *Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013) [57]; *Delfi v Estonia* App no 64569/09 (ECtHR, 16 June 2015) [120]–[122].
[47] European Data Protection Supervisor (Opinion 3/2018) Opinion on Online Manipulation and Personal Data at Page 20.

compliance with these codes also helps build transparency[48] . However, Page 30 of the report states that 'to encourage diverse debate, the government proposes to introduce a power for the DCMS Secretary of State to require the ICO to set up a panel of persons with relevant expertise when developing codes of practice, and complex or novel guidance'.

This is extremely concerning.

As flagged above, the regulator should be completely independent of any Parliamentary and political influence, including when developing Codes of Practice. The Independent Reviewer of Terrorism Legislation is an illustrative example: in *Big Brother* the ECtHR stressed that the uniqueness of the Reviewer's role lied in 'its complete independence from government'[49]. The UN Special Rapporteur's Report on Freedom of Expression stated that any law limiting the right to freedom of expression must be applied by a body that is independent of any political power in a way, which is not arbitrary, including the possibility of remedy and challenge [50]. Moreover, case law from the ECtHR states that, in a field where abuse was highly likely, it was also in principle desirable to entrust supervisory oversight to a judge[51]**.** Parliamentary scrutiny should be limited to ensuring the regulator fulfils its duties appropriately.

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**

Please refer to previous answer above ie Q5.5.2.

Q5.5.4. The proposals under this section 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**

As per page 130 of the report, the government proposes to provide the Secretary of State for DCMS a parallel power to that granted to the Houses of Parliament in section 125(3) of the Data Protection Act 2018 in the approval of codes of practice and new or complex guidance. This will provide the Secretary of State with a 40-day period to approve a code of practice or new or complex guidance. The report notes that if the Secretary of State does not approve it, the ICO cannot issue it and another version of codes of practice and new or complex guidance must be prepared. As explained above, the regulator should be completely independent of any Parliamentary and political influence, including when developing codes of practice and new or complex guidance. Thus, these proposals should not apply to a broader set of the ICO's regulatory products either**.**

[48] Article 29 Working Group Guidelines on Consent under Regulation 2016/679 at pg 19.
[49] *Big Brother Watch and Others v United Kingdom (*Applications nos. 58170/13, 62322/14 and 24960/15*)* at 160.
[50] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (16 May 2011) at Page 8.
[51] *Klass and others v Germany (*Application no. 5029/71*)* at Para 56 *Big Brother Watch and Others v United Kingdom (*Applications nos. 58170/13, 62322/14 and 24960/15*)* at Para 58.

Q5.5.5 Should the ICO be required to undertake and publish an impact assessment on each and every guidance product?

○ **Yes**

As noted above, this would help to build transparency, as well as being compliant with both, the ECHR and the Strasbourg Court's accessibility, foreseeability and rule of law principles.[52] Please refer to Q5.5.1.

5.6 Complaints

The government welcomes views on the following questions:

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**

Clearly, the ICO would benefit from a more proportionate regulatory approach to data protection complaints. However, it is arguable that the government's desire to establish a more efficient scheme by allowing the ICO to take a risk-based approach, focusing on upstream activities to detect and address problems, will also be a significant human rights issue. A risk-based approach entails establishing the scope or scale of risks associated with a specific case and a known threat. It is true that such an approach may be helpful in technical scenarios in which data controllers such as, corporate actors must assess their individual operational risks. However, the suggested risk-based approach would also have data controllers assessing their operational risks vis-à-vis data subjects' human rights. Similarly, data controllers would additionally have an interest in minimizing the risks to create products. It is thus arguable that a risk-based approach to regulation would not appear to align well with the protection of human rights on the internet such as, data subjects' right to protection of their personal data and privacy. It should be noted that the GDPR specifically refers to risks and sets out the conditions for carrying out a risk assessment under some circumstances. For example, if there is a data breach. Importantly, however, this piece of legislation is not only based on rights, but perhaps more significantly, making these rights operational[53]. Indeed, during the GDPR negotiations, the Article 29 Working Party warned that the risk-based approach should never replace corporate actors' duties to safeguard human rights:

'…the Working Party is concerned that both in relation to discussions on the new EU legal framework for data protection and more widely, the risk-based approach is being increasingly and wrongly presented as an alternative to well-established data protection rights and principles, rather than as a scalable and proportionate approach to compliance. The purpose of this statement is to set the record straight[54].'

---

[52] *Kennedy v the United Kingdom* App no 26839/05 (2010) 52 EHRR [151]; *Rotaru v Romania* App no 28341/95 (2000) 8 BHRC 449 [52]; *Liberty and others v the United Kingdom* App no 58243/00 (2008) 48 EHRR 1 [59]; *Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013) [57]; *Delfi v Estonia* App no 64569/09 (ECtHR, 16 June 2015) [120]–[122].

[53] https://www.accessnow.org/eu-regulation-ai-risk-based-approach/

[54] Article 29 Working Group Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks 2014/218 at page 2.

The above warning elaborates that 'rights granted to the data subject by EU law should be respected regardless of the level of the risks which the latter incur through the data processing involved'[55]. It is worth noting that, since then the data protection authorities have not changed their mind on this issue. In fact, the European Data Protection Board stresses that, pursuant to the GDPR, the risk-based approach is restricted to a limited number of articles and makes perfectly clear that other duties continue to be relevant[56]. In other words, to promote human rights standards, a more proportionate regulatory approach to data protection complaints should be a human rights-based law such as, the GDPR. Thus, the government should not jeopardize ECHR/CJEU human rights by replacing a simple risk mitigation activity by the very companies, which have vested interests in developing technologies such as, Artificial Intelligence[57] - see to that effect the high-risk AI systems included in the EU proposed AI Act[58].

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?

○ **Strongly disagree**

Again, the government's proposal to create a requirement for the complainant to attempt to resolve their complaint directly with the data controller before lodging a complaint with the ICO, would not seem to align well with current human rights instruments. For instance, in applying the rule of law principle, the Strasbourg Court has observed that executive authority interference with individuals' Articles 8 and 10 Convention rights must also be subject to effective supervision[59] (eg the ICO). Moreover, in *Tele2/Watson* the CJEU held that, considering both Article 8(3) of the EU Charter of Fundamental Rights and the Court's case-law, a crucial aspect about the protection of individuals concerning the processing of their personal data was prior review by the courts or independent authorities such as, the ICO[60].

Additionally, in *Delfi v Estonia*, judges Sajó and Tsotsoria observed that although governments did not always directly restrict human rights, the fact that - as in the current situation - they would seem to exert pressure and impose liability on data controllers meant that 'collateral or private-party censorship' was the unavoidable outcome[61]. For instance, these judges cautioned that the use of technical means led to a number of problems, such as intentional overbreadth and diminished procedural safeguards[62]. Moreover, crucially, they concluded that as data controllers would have to provide 'supervision 24/7', this would result in absolute and strict liability. In other words, 'blanket prior restraint'[63].

[55] Ibid at page 3.
[56] European Data Protection Board Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.
[57] https://www.accessnow.org/eu-regulation-ai-risk-based-approach/
[58] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
[59] *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [110]; *Rotaru v Romania* App no 28341/95 (2000) 8 BHRC 449 [59]; see also *Klass and others v Germany* App no 5029/71 (1979–1980) 2 EHRR 214 [55]; *Amann v Switzerland* App no 27798/95 (2000) 30 EHRR 843 [60].
[60] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsenk* [2016] All ER (D) 107 (Dec) and *Secretary of State for the Home Department v Tom Watson* [2016] All ER (D) 107 (Dec) [123].
[61] Joint dissenting opinion of Judges Sajó and Tsotsoria in *Delfi v Estonia* App no 64569/09 (ECtHR, 16 June 2015) [2].
[62] Ibid.
[63] Ibid [35].

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?

○ **Somewhat disagree**

Although having a simple and transparent complaints-handling process to deal with data subjects' complaints is always welcome, in view of the above answer, this question would not be directly relevant/applicable. As flagged above, executive authority interference with individuals' Articles 8 and 10 Convention rights should be subject to effective supervision[64] such as, the ICO.

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

In any case, if the government decided to introduce a requirement for the complainant to attempt to resolve their complaint directly with the relevant data controller, this should not apply to small and medium-size data controllers. This is because such a requirement would have a disproportionate impact on their freedom to conduct their business, under Article 16 of the EU Charter – see to that effect Article 17(6) of the EU Directive on Copyright in the Digital Single Market[65].

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**

As noted in Q5.5.1, in terms of building transparency, any regulatory proposal should always be fully in line with both, the ECHR and the Strasbourg Court's accessibility, foreseeability and rule of law principles[66]. Thus, although setting out in law the criteria, which the ICO could use to establish whether to pursue a complaint would certainly provide such clarity, it has already been suggested that, taking a more risk-based approach to complaints vis-à-vis a ECHR/CJEU human rights-based approach is highly problematic.

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**

---

[64] *Barbulescu v Romania* App no 61496/08 (ECtHR, 5 September 2017) [110]; *Rotaru v Romania* App no 28341/95 (2000) 8 BHRC 449 [59]; see also *Klass and others v Germany* App no 5029/71 (1979–1980) 2 EHRR 214 [55]; *Amann v Switzerland* App no 27798/95 (2000) 30 EHRR 843 [60].

[65] https://eur-lex.europa.eu/eli/dir/2019/790/oj

[66] *Kennedy v the United Kingdom* App no 26839/05 (2010) 52 EHRR [151]; *Rotaru v Romania* App no 28341/95 (2000) 8 BHRC 449 [52]; *Liberty and others v the United Kingdom* App no 58243/00 (2008) 48 EHRR 1 [59]; *Yildirim v Turkey* App no 3111/10 (ECtHR, 18 March 2013) [57]; *Delfi v Estonia* App no 64569/09 (ECtHR, 16 June 2015) [120]–[122].

As the report notes on page 134, the enforcement framework incorporated into both, the GDPR and UK Data Protection Act 2018 provides a combination of strong mechanisms for the ICO to enforce data protection legislation. This not only includes information notices requiring organizations to give certain information to the UK data protection authority, but also the ability to issue sanctions up to £17.5 million, or 4% of overall worldwide yearly turnover (whichever is higher). Indeed, the goal of the enforcement framework is to promote compliance and act in a proportionate and robust way. This is something which is entirely consistent with Recital 148 of the GDPR. It states that 'in order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation.' Similarly, in *Schrems II* the CJEU stressed that the primary responsibility of data protection authorities such as the ICO was to carefully monitor the implementation of the GDPR, as well as ensuring its enforcement[67].

Problematically, however, it has been convincingly argued that despite both, Recital 148 of the GDPR and *Schrems II*, it is particularly concerning that the ICO appears to have been overlooked a number of serious matters, resulting in data protection complaints lacking any real chance of a formal regulatory response[68]. It is worth noting that the vast majority of ICO's resources (around 75%) are currently being devoted to 'proactive engagement activities',[69] which leaves just around one quarter for enforcement purposes. Unfortunately, this is regardless of the stated fact that the ICO receives 'high numbers of public complaints'[70] regarding not only data protection, but also associated electronic privacy practices. For example, in a similar way to the previous year, in 2019-20 the ICO received around 40K data protection complaints,[71] in addition to approximately 128K concerns pursuant to the Privacy and Electronic Communications Regulations[72]. On the other hand, this contrasts with the ICO just invoking its formal enforcement powers in very rare occasions. To sum up, during the 2019-20 period, the ICO issued 'seven enforcement notices, four cautions and eight prosecutions and fifteen fines'[73]. Furthermore, most ICO's attention was paid to 'processing for direct marketing purpose', as well as 'data security shortcomings'[74].

Arguably, even if this is not regrettably the case, following Recital 148 of the GDPR the current UK enforcement regime should be broadly fit for purpose as it theoretically provides the ICO with strong mechanisms to promote compliance and to impose relevant sanctions. Thus, what the government should do is to look beyond introducing new powers to allow the ICO to perform novel supplementary functions and focus on monitoring that the ICO complies with its primary responsibility, namely, carefully supervising the application of the GDPR, as well as ensuring its enforcement – see to that effect *Schrems II* [108][75].

---

[67] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximilliam Schrems* [2020] ECLI:EU:C:2020:559 [108].
[68] https://committees.parliament.uk/writtenevidence/22916/pdf/
[69] https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83- certified.pdf, pg 35.
[70] Ibid, pg 48.
[71] Ibid, pg 50.
[72] Ibid, pg 67.
[73] Ibid, pg 35. Some of this action may have related to the Freedom of Information Act 2000 which clearly falls outside the scope of your inquiry.
[74] https://www.openrightsgroup.org/blog/ico-enforcement-two-years-after-the-gdpr/
[75] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximilliam Schrems* [2020] ECLI:EU:C:2020:559 [108].

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 disagree**

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

○ Whether there are any other risks or benefits you can see in this proposal

○ If you foresee any risks, what safeguards should be put in place

According to page 136 of the report, during the course of the ICO's investigations into alleged infringements of the data protection framework, the UK data protection authority has, in specific situations, experienced difficulties in obtaining sufficiently and timely detailed information from organisations concerning organisational and technical measures being put in place and any relevant remedial actions. Thus, the government is proposing to introduce a new power for the ICO to enable the commission of independently created technical reports to inform investigations.

Again, it is arguable that this is not required as pursuant to Recital 148 of the GDPR and *Schrems II*, the ICO has strong mechanisms not only to promote compliance, but also imposing proportionate, dissuasive and robust sanctions. On the other hand, as flagged above, what the government should do is to focus on monitoring that the UK data protection authority satisfies its primary responsibility. In other words, carefully screening the application of the GDPR, as well as ensuring its enforcement[76].

Indeed, it remains a matter of serious concern that, despite both, Recital 148 of the GDPR and *Schrems II*, as of today, the ICO seems to have failed to make any practically use of its enforcement powers under data protection framework. To serve as a case study, currently, the Digital Advertising Technology (AdTech) industry is seemingly systematically tracking, profiling and seeking to manipulate data subjects' behaviour, for purely commercial reasons, without requiring 'freely given, specific, informed and unambiguous' opt-in consent[77] - see to that effect Article 4(11) GDPR. In September 2018, Jim Killock and Dr Michael Veale complained to the ICO over its failure to take substantive action against what their own investigation found were very dangerous and widespread illegal practices regarding this issue[78]. In June 2019, the ICO's investigation concluded that the AdTech industry was violating the GDPR due to industry practices such as, gathering and sharing data subjects' browsing history without checking who may end up accessing this personal data[79]. Worryingly, however, regardless of such manifestly illegal practices, in September 2020, the UK data protection authority decided to close the investigation without taking any substantive action[80]. Moreover, during the first Covid-19 lockdown measures, the ICO also decided to

[76] Ibid.
[77] https://committees.parliament.uk/writtenevidence/22916/pdf/
[78] https://www.openrightsgroup.org/press-releases/privacy-organisation-open-rights-group-taking-the-privacy-regulator-ico-to-court-in-a-landmark-case/
[79] https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf The ICO's investigation concluded that: (1) Adtech companies collect and share people's browsing histories but have no practical control where this information ends up; (2) given this astounding lack of basic security, other rights such as consent access to data are unobtainable; (3) that the industry relies on spurious legal arguments to justify widespread poor practice.
[80] See correspondence between ICO and ORG, available on request to the ORG.

'pause' enforcement[81]. In November 2020, it was announced that the Open Rights Group was taking the ICO to court over the UK data protection authority's refusal to stop illegal practices by the AdTech industry[82].

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?

In view of the previous answers, this question would not be directly relevant/applicable.

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

In view of the previous answers, this question would not be directly relevant/applicable.

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 attend an interview in the course of an investigation?

○ **Strongly disagree**

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.

As the report notes on page 138, it is true that the ability to interview a specific person as part of an investigation could provide a key mechanism for collecting evidence. However, it is arguable that, pursuant to the Strasbourg Court's case-law, in a field where abuse is highly likely, it is in principle desirable to entrust supervisory oversight to a judge[83]. Indeed, even the government appears to acknowledge the risk of allowing the ICO to oblige witnesses to attend an interview during an investigation. The report clearly stresses that 'as this is a wide-ranging power with implications on individuals' rights and freedoms, any consideration of the granting of this power needs to be carefully evaluated' – see page 138.

It is worth noting that, in the UK summonses are included in Part 34 of the Civil Procedure Rules (CPR). This code regulates how civil (non-criminal) cases are considered in court. Importantly, however, according to Part 34 of the CPR, only the court has the authority to order a witness to appear in court to provide evidence on a specific time. Thus, if the ICO were to force any individual to appear in court it would have to apply to the court requesting the relevant judge(s) to issue such an order[84].

The main issue with witness summonses though, is that if the ICO were to force someone to appear in court, it may be unable to understand what they will say under cross-examination. It may be that, for some reason, they could be resentful towards the regulator because perhaps the ICO has compelled them to be there, thus they might not speak what it is expecting them to. On the other hand, it can be of great help if there is evidence the ICO directs the witness to, which demonstrates what took place at the time. In these cases, it

[81] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/05/ico-statement-on-adtech-work/
[82] https://www.openrightsgroup.org/press-releases/privacy-organisation-open-rights-group-taking-the-privacy-regulator-ico-to-court-in-a-landmark-case/
[83] *Klass and others v Germany (*Application no. 5029/71*)* at Para 56 *Big Brother Watch and Others v United Kingdom (*Applications nos. 58170/13, 62322/14 and 24960/15*)* at Para 58.
[84] https://www.samuels-solicitors.co.uk/news/forcing-someone-to-be-a-witness

would be harder for the witness to give evidence that conflicts with the documentary evidence[85].

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 disagree**

In view of the previous answer, this question would not be directly relevant/applicable.

The government welcomes views on the following questions:

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?

○ **Somewhat agree**

As the report notes on page 140, increasing the time permitted would make it possible for the UK data protection authority to provide organisations with more time to answer to their enquiries and the regulator more time to consider the relevant evidence. For example, in a similar way, there is no deadline for the Competition and Markets Authority to come to a conclusion on a final penalty.

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 disagree**

It has been reported that, for instance, in the US and Canada, stopping the clock is a controversial practice, which law makers tend to rely on in order to meet statutory or constitutional deadlines. For instance, Riddick's Rules of Procedure illustrates that 'the official clock is stopped by agreement of the 'powers that be' without any motion or announcement one minute before the designated hour'[86]. Moreover, it has also been reported that, often these 'stop-the-clock' mechanisms are adopted to permit more time for deal-making or lobbying to get the necessary votes for one side to succeed on a measure[87]. For this reason, the government proposal to introduce a 'stop-the-clock' mechanism if the requested information is not provided on time seems an unwelcome suggestion.

The government welcomes views on the following question:

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?

[85] Ibid.
[86] https://archive.org/details/riddicksrulesofp00ridd
[87] https://en.wikipedia.org/wiki/Stopping_the_clock#cite_note-2

○ **Strongly agree**

Please refer to Section 5.4 ‘Accountability and Transparency’ above.