Response to the Government's 'Data: A New Direction' Consultation[1]

Submitted by

Dr Jiahong Chen (University of Sheffield)
Dr Edward Dove (University of Edinburgh)
Professor Lilian Edwards (Newcastle University)
Dr Ansgar Koene (University of Nottingham)
Professor Derek McAuley (University of Nottingham)
Dr Anna-Maria Piskopani (University of Nottingham)
Dr Lachlan Urquhart (University of Edinburgh)

19 November 2021

This submission aims to address a selection of questions formulated in the government's 'Data: A New Direction' consultation document by presenting findings and views based primarily on research undertaken by us, although we have also drawn on publicly available sources[2]. As academics with expertise in the broader areas of data protection and technology regulation, we will focus specifically on three sections of the consultation: **research purposes (Section 1.2), reform of the accountability framework (Section 2.2) and privacy and electronic communications (Section 2.4).** We would be happy to be contacted for further evidence and for this submission to be published in full[3].

Research Purposes (Section 1.2)

Q1.2.1. To what extent do you agree that consolidating and bringing together research-specific provisions will allow researchers to navigate the relevant law more easily?

○ Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
◉ **Strongly disagree**

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

[2] This submission was supported by the EPSRC Grant Number EP/T022493/1.
[3] Any enquiries regarding this submission should be sent to : horizon@nottingham.ac.uk.

The data protection legislation, comprising the Data Protection Act 2018 and UK GDPR, is drafted in a way that promotes logical coherence and structure, largely moving from principles (e.g. Article 5 and Chapter 1 UK GDPR) to specific rules within specific sectors (e.g. Article 89 and Chapter 9 UK GDPR), including scientific research. The structure of the DPA 2018, with Schedules, is also drafted in a way that promotes logical coherence. To our knowledge, there is no robust evidence that supports the claim that the structure of the current legislation makes it difficult to realise the full benefits of the system, nor are we aware of any concerns within the research community that the current structure of the research-specific provisions is causing confusion and hurting research and innovation in any material way. The research community, on the whole, is aware of the relevant provisions in both the Data Protection Act 2018 and UK GDPR.

Before any restructuring takes place, careful consideration must be given to the effects, including incidental, this would have on data protection legislation as a whole, given the careful attention that has been given to drafting both primary pieces of legislation in a coherent manner. Details are also lacking as to what 'consolidation and bringing together' would entail for the research-specific provisions as currently drafted, and it is unclear if the government considers 'consolidation' as distinct from 'bringing together', given both phrases are used, and if so, what this means for the current provisions in the law, including Articles 9(2)(j) and 81 UK GDPR, and Section 19 DPA 2018. We also note that two of the 'research-specific' provisions cited in the consultation, viz. Articles 89 UK GDPR and Section 19 DPA 2018, are in fact specific provisions requiring appropriate safeguards that also cover processing of personal data that is necessary for archiving purposes in the public interest and processing of personal data that is necessary for statistical purposes.

Consolidating and bringing together the research specific provisions alone will not help researchers navigate the special regime for scientific research. Instead, having a continuous active role in engaging with those provisions will be more important. It would be most helpful if researchers were trained to learn their legal obligations and the risks of innovative research to human rights, exchange good practices, participate to the creation of codes of conduct, discuss ethical dilemmas, challenges and concerns with ethical committees and data protection authorities.

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

○ Strongly agree
○ Somewhat agree
◉ Neither agree nor disagree
○ Somewhat disagree
○ Strongly disagree

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

On the whole, we agree to some extent that creating a statutory definition of 'scientific research' would result in greater certainty for researchers. To our knowledge, there has not been any evidence that the absence of a definition in the data protection legislation has been a source of confusion or cause for concern, as data controllers have been able to consult Recital 159 to recognise that data protection legislation takes a broad, expansive, and flexible view as to what constitutes scientific research.

Nonetheless, given that data protection legislation contains provisions drafted with specific relevance to scientific research, a statutory definition would provide appropriate legal status alongside the operative provisions and improve transparency for data subjects. This said, creating a statutory definition of 'scientific research' would only result in greater certainty for researchers to the extent the definition is drafted with sufficient clarity and precision, and flexibility to

accommodate the future expansion of research realms. We therefore call for the government to further consult the scientific communities, as well as representatives of vulnerable groups who might be affected by such a change, before proposing any change to the definition.

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

◉ **Yes**
○ No
○ Do not know

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

We support the current definition of 'scientific research' as drafted in Recital 159 of the UK GDPR. In particular, we agree that it should be interpreted in a broad manner that includes, for example, technological development and demonstration, fundamental research, applied research and privately funded research, and studies conducted in the public interest in the area of public health. In particular, we support the definition which does not distinguish between scientific research pursuing public interests and that pursuing private or commercial research. This means that as long as UK domestic law (including data protection law) is met, primarily private or commercial interests can be pursued through the processing of personal data for scientific research purposes.

We also note that a recommendation from the Council of Europe (Explanatory Report of Convention 108) states that processing of data for scientific research purposes aims at providing researchers with information contributing to an understanding of phenomena in varied scientific fields (epidemiology, psychology, economics, sociology, linguistics, political science, criminology, etc.) in view of establishing permanent principles, laws of behaviour or patterns of causality which transcend all the individuals to whom they apply.

It should be made explicit that scientific research means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice. It is well-documented that the public is uncomfortable about sharing personal data to private bodies even in a research context,[4] especially in relation to sensitive data such as health data.[5] If safeguards in such circumstances are not made very apparent, patients will withdraw or falsify their data as the recent GPDPR opt-in controversy has clearly shown. We recommend that if a definition including private-sector research is codified in law, safeguards for such transfer should be explicitly provided at the same time. Where researchers in private-sector communities may not benefit from procedural and cultural safeguards, such as research ethics committees, it will be even more important to make sure that they are assured of their obligations.

Even worse, cases such as the Cambridge Analytica scandal have shown how research activities without the above-mentioned qualities can cause harm to society and democracy. Thus, those activities should be excluded from the scope of scientific research.[6] We challenge the idea that any

[4] See https://understandingpatientdata.org.uk/how-do-people-feel-about-use-data and https://www.hra.nhs.uk/about-us/news-updates/sharing-anonymised-patient-level-data-where-there-mixed-public-and-private-benefit-new-report/

[5] For findings from work by Ada Lovelace Institute, see https://www.adalovelaceinstitute.org/blog/the-foundations-of-fairness-for-nhs-health-data-sharing/

[6] For more examples, see https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf, pp. 7-9.

claims of 'innovation' are intrinsically of significant value, and believe true ingenuity requires novel ways of thinking outside the traditional business model of exploiting and monetising personal data.

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

○ Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
◉ **Strongly disagree**

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

We are not aware of any evidence from the research community, be it formally conducted empirical research or anecdotal communication, that the need for identifying a lawful ground for personal data processing for research purposes creates barriers for researchers. We have not been made aware of any concerns from the research community that they face uncertainty determining lawful grounds for processing personal data under the existing framework of Article 6(1) UK GDPR. Moreover, it is our view that to remove this legal obligation would create significant risk for researchers in terms of sustaining participation of data subjects in research activities and in protecting and promoting public trust in research, as this obligation adheres to the data protection principles of lawfulness, fairness, and transparency. We therefore are of the view that researchers ought to continue to identify a lawful ground for personal data processing for research purposes.

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

○ Strongly agree
◉ **Somewhat agree**
○ Neither agree nor disagree
○ Somewhat disagree
○ Strongly disagree

Please explain your answer and provide supporting evidence where possible.

It is our understanding that almost all, if not all, (public) universities in the UK have since May 2018 been clear in identifying Article 6(1)(e) as the relevant lawful basis for personal data to be processed in relation to a 'university research project', which we understand to mean a data processing activity conducted by academic staff or students or other persons engaged by the university in relation to the data processing activity. We are not aware of any universities having difficulty with interpreting this legal basis or of any uncertainty caused by this provision such that burdens for research have arisen or that useful research has been discouraged in any way. This said, provided the clarification in legislation is not overly prescriptive and inflexible, this proposal would likely be welcome by universities and not raise additional risk to data subjects or the coherence of data protection legislation. It remains to be seen what the government envisions in terms of detail for when universities can rely on this lawful basis. We suggest that were the government to legislate to this effect, it be done as additional text to Section 8 of the DPA 2018.

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

○ Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
◉ **Strongly disagree**

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

We note that the European Commission's original proposed text for the GDPR in January 2012 included a provision at Article 6(2) that stated: 'Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83 [now Article 89].' This proposal did not survive the trilogue negotiations, and ultimately, what remains in data protection legislation is the scientific research exemption for processing special category data under Article 9(2)(j). There was uncertainty about the scope and meaning of this original proposal from the Commission (which we understand was supported by the Council), including why it was placed as a separate paragraph under Article 6, rather than within the paragraph covering different lawful bases under Article 6(1), and whether it was narrower in scope than the special data category exemption for scientific research under Article 9(2), which if so, would create uncertainty and logical incoherence. Given this historic uncertainty was never satisfactorily resolved, we do not see the benefits of introducing a new legal basis under Article 6(1) - assuming this is where the new ground would be introduced - as outweighing the drawbacks this would create for both researchers and data subjects, including concern about maintaining adequacy with the EU/EEA, which is crucial for maintaining the UK's reputation as a world leader in research (given our beneficial ties with European collaborators on many research projects across different fields of research).

Beyond the concern that this new lawful ground may create greater uncertainty for researchers rather than certainty, it is unclear: (a) how this new lawful ground would interact with the existing special category for scientific research under Article 9(2)(j); (b) how this would interact with existing lawful grounds that are commonly used for scientific research, specifically Article 6(1)(e) for public bodies and Article 6(1)(f) for commercial organisations; and (c) what suitable safeguards would be in place, in addition to those already present in Article 89(1), to make sure this new lawful ground was not abused. (We note that consent is not commonly relied upon for scientific research, and indeed is not encouraged by bodies such as the Health Research Authority as the appropriate lawful ground for scientific research.[7])

Our concerns are heightened given that 'scientific research' is understood to have a large meaning that encompasses commercial/privately funded organisations, not to mention research conducted by 'citizen scientists' (i.e. those undertaking research activities in their home and who may not have the benefit of institutional knowledge and infrastructure such as research ethics committees and guidelines[8]). A new legal basis to process personal data for scientific research would in principle be available to these organisations.

[7] See Chen J, Dove ES & Bhakuni H. Explicit Consent and Alternative Data Protection Processing Grounds for Health Research. doi: 10.31235/osf.io/4fdsj

[8] See Dove ES, Chen J. To What Extent Does the EU General Data Protection Regulation (GDPR) Apply to Citizen Scientist-Led Health Research with Mobile Devices? The Journal of Law, Medicine & Ethics. 2020;48(1_suppl):187-195. doi:10.1177/1073110520917046

We know from long-standing empirical research conducted in the UK (by groups such as Understanding Patient Data) that the public is more sceptical of research involving their personal data when the controller is a commercial organisation. A new, separate legal basis for scientific research, if drafted broadly and without suitable, robust safeguards in place, could lead to misuse and severe undermining of public trust. Indeed, even a well-meaning aim to enable more data processing for scientific research, and subject to appropriate safeguards, could create risk of undermining trust-building exercises with the public and eroding researchers' social licence to operate, i.e. to process personal data in the absence of data subjects' consent yet still with data subject and public support. For these reasons, we largely do not agree with the proposal for a new, separate lawful ground for research.

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

In the context of health research, were the government to proceed with a new, separate lawful ground for research (despite our concerns in doing so, as noted above), appropriate safeguards should include, foremost, research that has been approved by research ethics committees. This means a research ethics committee recognised or established by or on behalf of the Health Research Authority under the Care Act 2014, or any other group of persons which assesses the ethics of research involving individuals and which is recognised for that purpose by or on behalf of the relevant Ministers in the UK Government or across the Devolved Administrations, or by a higher education institution (which itself is defined appropriately). The concern here is that in the absence of research ethics committee approval, be it a higher education institution REC or NHS REC, there will be inadequate safeguards in place to enable data processing to take place under this ground.

This is, again, especially of concern for scientific research conducted within commercial organisations or by 'citizen scientists' who may not have a research ethics committee to submit their research application to (as with a university) or involve NHS patients or staff, thereby involving an HRA/NHS research ethics committee. Yet, to enable such organisations or persons to rely on this new, separate legal ground without accompanying research ethics committee creates significant risk for data subjects and public trust, particularly with respect to the ethical and lawful processing of personal data.

Among other safeguards necessary are that to rely on this new, separate legal ground, it should be demonstrated the scientific research purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject; *and* data enabling the attribution of information to an identified or identifiable data subject is kept separate from the other information as long as those scientific research purposes can be fulfilled in this manner.

In other areas of research, such as historical or social research, the safeguards required might differ. In general terms, the government should also consider additional approaches such as relevant sectoral standards of methodology and ethics, including the notion of informed consent, accountability and oversight, with a view to encouraging research activities that are in line with the aim to promote society's collective knowledge and wellbeing, as opposed to primarily serving private interests.

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

○ Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
◉ **Strongly disagree**

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

As noted above, it is relatively uncommon that researchers will rely on consent on the relevant legal basis to process personal data under Article 6(1), and bodies such as the Health Research Authority actively discourage researchers from doing so.[9] This is because withdrawal of consent could undermine types of scientific research that require data that can be linked to individuals. It is also because of challenges fulfilling the stringent conditions of consent under Articles 4(11) and 7 UK GDPR, and the challenges secondary users of data would face if data is originally collected under previous research on the lawful basis of consent. This is the principal reason why the scientific research exemption exists under Article 9(2)(j) and why regulators encourage controllers to rely on a lawful basis other than consent under Article 6(1). Thus, from a practical standpoint, allowing data subjects to give broader consent to future scientific research will have limited utility in the scientific research context, and may instead open up risks of leakage and abuse of data especially in the private sector which as discussed above may lack the stringent professional, ethical and organisational safeguards of traditional public-interest research.

This said, we can see some (limited) benefit to clarifying the form and function of broad consent in data protection legislation, with respect to scientific research, as Recital 33 seems to indicate. However, we mainly see a danger that consent might be treated as a form of proxy, blanket consent by data subjects for controllers to process their personal data in an unlimited variety of manners, under the guise of research, and for an indefinite period. Broad consent must be subject to robust, ongoing governance oversight, and in the research context, that includes research ethics committee approval, the need to establish that the scientific research purpose would be in the public interest, and ongoing transparency obligations by controllers to data subjects. Recital 33's reference to '...when in keeping with recognised ethical standards for scientific research', although somewhat ambiguously drafted, has been interpreted to mean, among other things, research ethics committee approval and ongoing transparency obligations by controllers to inform data subjects as to when personal data will be processed for a new specified scientific research purpose.

As the European Data Protection Board has noted in its Guidelines 05/2020 on consent, when research purposes cannot be fully specified, a controller must seek other ways to ensure the essence of the consent requirements are served best, for example, to allow data subjects to consent for a research purpose in more general terms and for specific stages of a research project that are already known to take place at the outset. As the research advances, consent for subsequent steps in the project can be obtained before the next stage begins. Yet, such consent should still be in line with the applicable ethical standards for scientific research. Moreover, it is expected that controllers still apply further safeguards in such cases, such as data minimisation, anonymisation, and data security. Transparency is an additional safeguard when the circumstances of the research do not allow for a specific consent; this means providing data subjects with regular updates on the research so data subjects have a basic understanding of the state of play and allow them to assess whether or not to use, e.g. the right to withdraw their consent. Finally, having a comprehensive research plan available for data subjects to take note of, before they consent, can help to compensate for a lack of purpose specification.

[9] See Chen J, Dove ES & Bhakuni H. Explicit Consent and Alternative Data Protection Processing Grounds for Health Research. doi: 10.31235/osf.io/4fdsj

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

○ Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
◉ **Strongly disagree**

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

While the data protection legislation does not, under Article 5(1)(b) or Article 6(1) UK GDPR, explicitly state that further use of data for scientific research purposes passes the lawfulness test under Article 6, we note that any inclusion and formal recognition of explicit statement in data protection legislation ought to consider the implications of this for research conducted by commercial organisations and 'citizen scientists', given the evidence that various studies conducted in the UK have shown regarding public scepticism and wariness of use of their data for scientific research purposes by the former, and inherent uncertainty with risk associated with the latter.

Clarification would be needed regarding, *inter alia*, whether this applies exclusively to the same data controller processing personal data, or other data controllers with whom the original controller shares the data; and whether disclosing personal data to a subsequent controller for scientific research purposes is always compatible further processing (and necessitates the subsequent controller to have its own legal basis for the processing). We also note the proposals for extension of further processing under Section 1.3 in this consultation, including reuse of data by a new data controller for new purposes; and although we are not here providing a full answer to questions in that section, for the avoidance of doubt, if this was also applicable to research processing, we would still require further evidence of safeguards, especially in the private and 'citizen science' sectors.

We also note that compatibility is only one element for the legitimacy of further processing. It also needs to fulfil the requirements of Article 5(1), i.e. to be transparent, fair and have a legal basis according to Article 6(1), as well as the other data protection principles of Article 5. Even though processing for research purposes (including data disclosure to a subsequent controller) were always considered compatible from the perspective of purpose limitation, the conditions for a valid legal basis under Article 6(1) should still be fulfilled.

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 agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
◉ **Strongly disagree**

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

We are concerned that the government is conflating a duty to provide information to data subjects with a duty to contact data subjects. We note that Article 12(1) stipulates that 'The controller shall take appropriate measures *to provide any information* referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information *shall be provided in writing, or by other means, including, where appropriate, by electronic means*. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means' (emphasis added).

This information provision obligation does not mean, as is suggested in paragraph 49(b) of the consultation, that controllers have a requirement 'to contact data subjects'; rather, they have an obligation provide information in a concise, transparent, intelligible and easily accessible form, and that may be accomplished by electronic means such as provision on a website. This means that data subjects must be informed of the details of the processing activity, which is one of the conditions of fair processing, and is a *sine qua non* for transparency. This information is usually contained in a notice, statement or policy. We note, too, that the Article 29 Data Protection Working Party has made it clear that, under Article 13, a controller must be proactive in providing the information to a data subject, meaning that 'the data subject must not have to take active steps to seek the information covered . . . or find it amongst other information, such as terms and conditions of use of a website or app'.[10] This, however, is not to be conflated with a duty to contact each individual data subject.

In consequence, data controllers that must provide additional information to data subjects if they intend to further process personal data for a purpose other than that for which the personal data were originally collected is an obligation that requires provision of information rather than an obligation to contact data subjects directly. Thus, we are not of the view that this is an obligation that requires significant time and resources such that it would 'lead to research being unviable'. We are concerned that replicating the Article 14(5)(b) in Article 13 would significantly risk undermining data subject rights and undermine public trust in research.

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

In light of our above concerns, we are not in favour of this Article 14(5)(b) exemption being applied to Article 13 under any circumstances.

Reform of the Accountability Framework (Section 2.2)

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'?

○ Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
◉ **Strongly disagree**

[10] https://ec.europa.eu/newsroom/article29/items/622227

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

We feel strongly that there is no incompatibility between a data protection regime which is flexible and risk-based, and one with a robust and detailed accountability framework. Furthermore, we strongly challenge the apparently pejorative labelling of some of the current legal requirements as 'prescriptive'. A flexible and risk-based accountability framework does not mean that specific compliance requirements are not needed, nor that they should be entirely up to data controllers to decide. The (UK) GDPR is often referred to by some industrial stakeholders as 'red tape', which largely ignores how the current legal framework has significantly improved the level of data protection in the UK, and brought about a cultural change of treating personal data more seriously. While there is indeed scope for improving the accountability framework to reduce unnecessary bureaucracy and strengthen future-proofness, the priority should be supporting sector-specific accountability requirements and best practices, rather than removing the existing legal requirements.

There are a number of problematic assumptions underpinning the desire to reform the accountability framework and contradictions, where on the one side the government commits to strong data protection and creating a world leading environment for innovation, yet on the other, seeks to remove key safeguards which guarantee these. The accountability principle is at the core of good data protection governance. The idea that innovation and data protection are in opposition creates a false dichotomy. If anything, data protection requirements should be viewed as prompts for more innovative data processing system architectures, such as the decentralised models we have pioneered in our research under the Databox project[11], and novel approaches to demonstrating compliance, as opposed to being labelled 'unnecessary burdens' (para 139).

We note furthermore that many businesses who might claim to benefit from the removal of 'red tape' will in fact operate across multiple markets and find that to enter those, they still have to comply with EU accountability standards. This may also be true of many non-EU markets where the GDPR has been taken up as a global 'gold standard'. Thus, in fact any relaxation of so-called 'prescriptive' standards may make little different to most sectors of UK-operating business, and create uncertainty as to exactly what is required among the rest.

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'?

○ Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
◉ **Somewhat disagree**
○ Strongly disagree

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

○ ***Please share your views on whether a privacy management programme would help organisations to implement better, and more effective, privacy management processes.***

○ ***Please share your views on whether the privacy management programme requirement would risk creating additional burdens on organisations and, if so, how.***

The Accountability Principle, as framed in GDPR, is deceptively simple where it requires a demonstration of compliance with Article 5(1) GDPR (the data protection principles such as data minimisation, security, lawful processing etc). However, read in conjunction with Article 24 GDPR,

[11] See https://www.horizon.ac.uk/project/databox/ .

it hints towards the full remit of what accountability requires, which is the data controller to provide a demonstration of accountability not just with Article 5(1) data protection principles, but arguably the entire GDPR. Thus, accountability is central to GDPR compliance more widely, which the document recognises itself (para 144).

A privacy management programme can be beneficial for some organisations, but not necessarily all of them. Our empirical work engaging with the IoT industry, for example, has uncovered that the legal barriers encountered by organisations include 'the current regulatory framework […] being one-size-fits-all, lagging behind reality, lacking baseline requirements and reliant on private enforcement'.[12] A privacy management programme may address some of those challenges for some organisations, but may make others worse. For example, without setting out the minimum compliance requirements supported by strong enforcement, mandating privacy management programmes will expose organisations to grave legal uncertainties with regard to their data protection duties. For many organisations, especially SMEs, following clear, specific, actionable safeguards provided by law or sector-specific initiatives is a less burdensome approach for them.

It should also be noted that some key elements of privacy management programmes are already covered by legal requirements under current data protection law. In the consultation document, the government envisages that a privacy management programme will cover 'leadership and oversight, risk assessment, policies and processes, transparency, training and awareness of staff, and monitoring, evaluation and improvement.' Most of these elements are however required under a proper interpretation of the relevant provisions in the UK GDPR, including data protection by design and by default (Article 25, noting the concept of 'organisational measures'), data protection impact assessment (Article 35, noting the risk assessment and review requirements), and transparency safeguards (Articles 12-14).

If the response to accountability tends towards a box ticking exercise, that misses the point of accountability. In part, it is not just a series of steps to be taken, but instead a more holistic drive to embed a culture of accountability around data protection in the organisation, and to find mechanisms of demonstrating this. It is concerning that the claim is that by focusing on accountability, which is at the heart of GDPR compliance, it is 'misdirecting time and energy away from activities that ensure responsible use of data'. It contradicts the ICO's framing of accountability, which foregrounds the cultural value of promoting data protection: 'It's a real opportunity to show that you set high standards for privacy and lead by example to promote a positive attitude to data protection across your organisation.'[13] In general, current ICO guidance on accountability reiterates the importance of leadership in organisations around DP, that it is not a box ticking exercise, that there is not a one-size-fits-all approach. It already uses language of privacy management programmes (existing within the current accountability framework). Hence it is unclear what the step change the government's proposal would add, and if the UK seeks to be a leading location for innovation globally, lowering regulatory standards does not seem to be a good approach for ensuring sustainable growth, maintaining adequacy for market access to EU and setting standards to be aspired to globally.

Considerations of types of data, processing, volume and sensitivity should *already be* factors that responsible data controllers are considering in defining the purposes of their data processing activities (para 151). For organisations that are already compliant with these requirements, mandating privacy management programmes will add further burdens on them. For those that have not fully complied, there is no reason to believe a privacy management programme will change

[12] Chen J & Urquhart L, 'They're all about pushing the products and shiny things rather than fundamental security':Mapping socio-technical challenges in securing the smart home, Information & Communications Technology Law, doi: 10.1080/13600834.2021.1957193

[13] https://ico.org.uk/for-organisations/accountability-framework/

their conduct; quite the contrary, it might actually risk giving them a free pass to carry on with the current practices by adopting a superficial programme. Overall, it would be a more effective strategy for the government to concentrate resources to enforcing the current legal requirements.

Further, a key strength of the accountability principle is its flexibility. On consulting ICO guidance, the types of activities that could be under the remit of demonstrating accountability become clear. But it is not prescriptive in what has to be used, when, and how. The principle is already flexible in terms of who a demonstration is owed to, although the data subject, and regulator are two clear stakeholders. Thus, controllers have a large degree of discretion in demonstrating how they comply with GDPR already.

The call for more innovative practices to support accountability are welcome, but it is unclear why this cannot occur within the existing accountability framework. Beyond rebranding of the 'privacy management programmes' it is difficult to see how this approach is qualitatively different to the current accountability mechanism. What would be more useful to businesses would be the government funding generation of a repository of best practice approaches, to show how, in concrete terms, different sectors and organisations have been complying with the accountability principle in novel, ICO-approved ways.

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'?

○ Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
◉ **Somewhat disagree**
○ Strongly disagree

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

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

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

As mentioned, a privacy management programme is not a panacea that will improve data protection compliance for all organisations. In that regard, in some cases individual data subjects might suffer from a lower level of data protection caused by the replacement of baseline compliance requirements with a privacy management programme. Loss of harmonisation across how UK organisations comply would have competitive impacts for different sizes of organisations. Para 141 of the consultation document says controllers can keep current mechanisms if they work, but others can adopt new ones if they prefer. Given the GDPR seeks to harmonise practice across Europe as a Regulation, this lack of level playing field across businesses is concerning for data subject interests and organisations with differing levels of organisational resources to dedicate to data protection. It could legitimise a lowering of standards, and less responsible practices, which could see consumers/data subjects suffer as a result (or 'beware').

In general, it remains unclear what the benefits of the privacy management system are over the existing accountability framework. The existing rules are balanced and attend to the needs of data subjects. The proposed changes appear to diminish safeguards for data subjects, and prompt a culture of more laissez faire, unharmonised approaches to data protection by controllers. There is a risk of legitimising a 'race to the bottom' instead of following the spirit of GDPR in trying to raise

standards around data protection compliance. Given the flexibility in the current accountability regime, these proposed shifts attempt to rebrand existing measures, in a weaker form and the balance of interests between data subjects and controllers is moving towards a business-friendly direction. This framing of how to encourage innovation neglects seeing good data protection governance as a gateway to improving businesses' position in the marketplace. By framing data protection obligations as burdens, and negative obligations, it neglects the possibilities for innovation in how companies satisfy these obligations. Instead, it would be encouraging for the government to provide examples of best practice, how companies have gone beyond viewing accountability as a box-ticking exercise and provided novel mechanisms to demonstrate compliance. As Urquhart, Crabtree and Lodge have argued, the architecture of a system and components within that can help demonstrate accountability.[14] Technical responses to demonstrating compliance will have a growing role, particularly by aligning the accountability principle with data protection by design and default requirements in Article 25, and Article 24 requirements on controllers to utilise organisational and technical measures to demonstrate their compliance with GDPR. Technical approaches to demonstrating accountability are a route where innovation and higher standards of data protection can co-exist, alongside interest in 'data intermediaries' (e.g. in para 129). The emphasis of the government should be on encouraging this type of innovation, in conjunction with the spirit of the accountability principle, as opposed to framing it as something that is a burden on innovation.

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'?

○ Strongly agree
○ Somewhat agree
◉ **Neither agree nor disagree**
○ Somewhat disagree
○ Strongly disagree

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

While some organisations might be struggling to appoint a suitable data protection officer (DPO), it is not necessarily the case across the board. In any event, just because some data controllers are unable to make suitable appointments does not mean that they should not.

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

○ Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
◉ **Strongly disagree**

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

[14] Urquhart L, Lodge T & Crabtree A, Demonstrably doing accountability in the Internet of Things, International Journal of Law and Information Technology, Volume 27, Issue 1, Spring 2019, Pages 1–27, doi: 10.1093/ijlit/eay015

We are not aware of any evidence that either public or private sector organisations find it difficult to integrate the functionality of the DPO. The consultation is misleading in implying that a DPO needs to be 'appointed' as a new or partial post within the organisation. Art 37(6) makes it clear that DPO duties can be outsourced and indeed a number of law firms already offer 'DPO-as-a-Service' – hence even for small businesses this can be managed just like other business compliance requirements.

Even if it were true that some organisations have difficulties appointing suitable DPOs, it does not follow that the requirement to appoint one should be removed. DPOs play important roles both internally and externally in supporting organisations to adhere to high standards of data protection. The public-facing functions of a data protection officer, such as handling complaints from data subjects, are a key part of ensuring individuals have effective access to exercising their rights. Requiring a named person to be responsible for data protection-related matters also reduces the risk of responsibility diffusion. DPOs are also vital to helping organisations conduct DPIAs where appropriate, whose removal we strongly oppose.

The government proposes the removal of the data protection officer who is meant to have certain attributes or skills, and replacement with a 'responsible person' who the organisation has wide discretion to define those skills or attributes that they will have. This is likely to lead to abuse and does not encourage a culture where data protection compliance is valued. Further, this may open to removing harmonisation across sectors and organisations, which, given the need to aim for high levels of compliance, strikes us as an unusual move and one to be resisted.

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

The relevance of this question is not immediately clear to us. It seems to suggest that it is desirable for organisations to maintain a similar role, and if that is the case, there is no reason in the first place for policymakers to disincentivise such a practice by making it no longer mandatory. On the other hand, if policymakers do not believe appointing a data protection officer is helpful, it is then unclear why it would matter whether organisations would maintain the role or not.

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**
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
○ Strongly disagree

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

A data protection impact assessment (DPIA) has a number of important functions for organisations dealing with personal data. Notably, it provides a compliance incentive (and sometimes mandate) for organisations to systematically review the impact of their data processing activities and to come up with measures to mitigate the negative impact. It also documents the key aspects of the decision-making process, not least the key data protection factors considered by the organisation, which serves as a key record for stakeholders to review, verify and challenge the claims made by the organisation. Requiring a prior impact assessment also supports organisations to develop the mindset of treating data protection as part of an integral part of their strategic plans, rather than

simply an afterthought. In this regard, a DPIA is one of the most important *ex ante* mechanisms under the current legal framework to promote the practice of identifying and minimising risk before conducting any data processing activities.

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 agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
◉ **Strongly disagree**

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

We are strongly opposed to the removal of DPIAs. Indeed, we are not aware of a general demand for their removal from business or the public sector and the consultation does not evidence such. In terms of pure value, for businesses, DPIAs may well save considerable expenditure in the long term, as well as preventing reputational losses from data breaches. The ICO is often willing to help in assessing risks within such a document and has provided exceptionally useful templates which we have seen used by non-lawyers with great success. Issues foreseen and risks mitigated as part of a DPIA will be taken into account in any later enforcement actions. They are a valuable tool for small businesses without legal counsel to spot risk and fend off pitfalls, not an overhead. In this sense they are more like a health and safety assessment for data than pointless red tape.

For the public sector, the value of DPIAs in promoting a sense to the public that their interests are being taken into account and their rights respected, that future harms are being anticipated and alternative, and that more privacy-friendly ways to achieve the delivery of public services are being considered, cannot be understated. This has been particularly apparent during COVID-19 where published draft or final DPIAs have often been the only way for the public and civil society to scrutinise vital technologies affecting crucial freedoms such as contact tracing apps and vaccine passports. In AHRC-funded work carried out by a consortium led by the British Institute of International and Comparative Law, to be published on 22 November 2021[15], researchers have found that apps and technologies used for public purposes during COVID have suffered from a lack of democratic scrutiny in both the legislature and the courts. This democratic scrutiny gap is only met, if at all, by freedom of information requests (often repelled under the policy exemption) and DPIAs. This may not be the first purpose of DPIAs but it is an extremely valuable one.

Finally, removing the DPIA requirement will significantly undermine the level of data protection in the UK, which might in turn jeopardise the UK's reputation as a safe destination for cross-border data transfers, and indeed any international arrangements recognising that status. A DPIA is not a perfect risk assessment tool, but it continues to support organisations to identify and minimise risks and wider negative impact associated with the use of personal data.

The proposed adoption of privacy management programmes should be discussed as an addition to – rather than a replacement of – the DPIA requirement under certain circumstances. We would like

[15] See Bingham Centre for the Rule of Law. (Forthcoming). The Role of Good Governance and the Rule of Law in Building Public Trust in Data-Driven Responses to Public Health Emergencies. Available at: https://binghamcentre.biicl.org/projects/the-role-of-good-governance-and-the-rule-of-law-in-building-public-trust-in-data-driven-responses-to-public-health-emergencies

to see consideration given to how to possibly integrate DPIAs with equality impact assessments and other impact assessments and to cover other important public interests such as group rights of privacy and other human rights. We propose the government finds an appropriate independent, expert and evidence-driven forum to investigate this, such as the Law Commission.

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.

The fact that few organisations approach the ICO for prior consultation is not necessarily an indication that this mechanism fails to achieve its objective. Under Article 36, organisations are required to consult the ICO only if their DPIA result suggests a high risk. Organisations with such a DPIA result may have simply decided not to proceed with the planned activities or have taken additional measures to mitigate the risk, so there is no need to consult the ICO anymore. As such, the prior consultation requirement may serve as a deterrent mechanism, and the case might be that it has indeed deterred high-risk activities, hence resulting in a low number of organisations ending up having to consult the ICO.

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

○ Strongly agree
○ Somewhat agree
◉ **Neither agree nor disagree**
○ Somewhat disagree
○ Strongly disagree

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

Under the current regime, organisations are already required to consult the ICO, and the fact that few organisations are taking this approach may be a consequence of: (a) some organisations have taken additional measures to mitigate the risk; or (b) some organisations have chosen not comply with this requirement and simply proceed with the high-risk activity without consulting the ICO. In either case, making the prior consultation voluntary would not provide additional incentives for the organisation to approach the ICO. Again, enforcement of the current rules against non-compliance with the prior consultation requirement should be the government's priority. Further, by removing this requirement, scope for harms to data subjects increases, and uses of high-risk processing technologies could be legitimately used, leaving little recourse for those whose data has been impacted by high risk uses that should never have been allowed in the first place (e.g., applications like live automated facial recognition).

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 agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
◉ **Strongly disagree**

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

Similar to the proposal to remove the DPIA requirement, there is no compelling evidence to suggest that the record keeping requirements are disproportionately burdening organisations. Record-keeping is a key part of holding data controllers accountable, and is indeed recommended as a good accountability practice by the CIPL report cited by the government. It is hard to see why record keeping around data processing, which should be best practice in any organisation, is objectionable. The new measures proposed in the privacy management programme i.e., 'what personal data is held, where it is held, why it has been collected and how sensitive it is') seem to streamline what information will be retained, but lack key information on important safeguards which pertain to good, secure record keeping. For example, under Article 30, it requires logging security provisions in place. This is a key safeguard in keeping sensitive information secure, and indeed a good governance practice by the controller. Removing the need to document how long it will be kept again erodes a key element in ensuring purpose limitation and data minimisation, key data protection tenets.

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?

○ Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
◉ **Strongly disagree**

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?***

Similar to the proposal to remove the DPIA requirement, there is no compelling evidence to suggest that the current breach reporting requirements are disproportionately burdening organisations. Without strong evidence to support doing so, shifting the data breaches notification threshold may risk sending the wrong message that data breaches are not taken seriously in the UK.

The call for ICO developing guidance on what is a material/non-material risk is welcome, and would help controllers determine if they need to notify or not. We are of the view that supporting controllers to better understand risks through ICO support is a better approach to protect the interests of data subjects, instead of removing the obligation to report, which may encourage a culture of under-reporting, and harms that could stem from this, both culturally in terms of organisations taking breaches less seriously, but also in terms of preventing direct and indirect harms to individuals e.g., loss of financial details etc.

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.

○ Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
◉ **Strongly disagree**

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

The ICO has been criticised for the lack of strong enforcement actions against violations of data protection law. Introducing the proposed voluntary undertakings process will only further undermine the UK's international reputation in terms of upholding a high standard of data protection by an independent data protection authority.

The government welcomes views on the following questions, relating to alternative reform proposals should privacy management programmes not be introduced:

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

○ Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
◉ **Somewhat disagree**
○ Strongly disagree

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.

The record-keeping requirements under Article 30 are different from the transparency requirements under Articles 13 and 14 in that the former is more externally facing, aiming to empower data subjects, whereas the latter is more internally facing, primarily serving as accountability safeguards and to facilitate compliance and investigation. Also, the overlap between different parts of the legal framework is not necessarily something undesirable. It could actually mean a more consistent approach to both external communication and internal documentation, minimising compliance costs for organisations.

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?

○ Strongly agree
○ Somewhat agree

◉ **Neither agree nor disagree**
○ Somewhat disagree
○ Strongly disagree

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

It is not clear what evidence the government has to support the claim that at the moment, data breaches are being over-reported. Even if that were the case, the risk of under-reporting is far more serious than over-reporting, and thus, any proposed adjustments to lower the reporting threshold must be justified on a compelling ground. We welcome the suggestion of encouraging the ICO to produce guidance on what falls within the scope of Article 33, but that does not require adjusting the current threshold.

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?

○ Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
◉ **Strongly disagree**

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

Our answer to Q.2.2.5 also applies to public authorities. If anything, public authorities are typically better-resourced than SMEs to recruit a suitable data protection officer, and their data processing activities are more likely to have more serious implications for the rights and freedoms of data subjects. In that regard, there is an even weaker justification for the removal of this requirement.

Privacy and Electronic Communications (Section 2.4)

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'?

There is some considerable work done on this topic in the EU as part of the legal reform of the ePrivacy Directive. One proposed change in the draft ePrivacy Regulation is to allow cookies for web-audience measuring purposes without user consent, which is largely what would fall within the definition of 'analytics'. It should however be noted that the EDPB and the EDPS have expressed concerns about the overly broad definition of web-audience measuring under the legislative proposals.[16] Some of those concerns are also relevant to the UK's proposed reform on data protection law, and we believe the scope of analytics should be limited to the following activities:

- First-party cookies that are solely used for providing low-level statistics of the use of the service, and that cannot contribute to or be combined with other tracking devices placed by the operator; notably, the use of IP addresses and other information provided by the user ('profile data') should be strictly limited to the purpose of basic demographic classification that does not allow singling out of the user.

[16] https://edpb.europa.eu/system/files/2021-03/edpb_statement_032021_eprivacy_regulation_en_0.pdf; https://edps.europa.eu/sites/default/files/publication/17-04-24_eprivacy_en.pdf

- Third-party cookies that fulfil all the conditions set out above for first-party cookies, and that are used only for the statistics of the use of the first-party service, and cannot be combined with the statistics or other purposes for the third-party operator or any other parties.

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 agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
◉ **Strongly disagree**

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

While we agree that analytics cookies, if strictly defined, can be exempted from the requirement of prior consent, users should be given the option to opt out of the use of analytics cookies, something sometimes known as 'opt-out consent' or 'implied consent'. This is because while analytics cookies, where appropriately deployed, are relatively low-risk compared to tracking cookies for example, some user groups may still prefer not to be 'counted' when they visit specific types of websites. The legitimate interest of the service provider in using analytics cookies does not justify not giving users the possibility to opt out of such analytics activities.

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

○ Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
◉ **Somewhat disagree**
○ Strongly disagree

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

We are concerned that expanding the scope of consent exemptions would further exacerbate the ongoing abuses of tracking technologies on the internet. We can see that there are scenarios where the service provider has an overriding, legitimate interest in placing cookies on the user's terminal device. Indeed, the ICO has envisaged a range of these cases, some of which can even fall within the scope of 'strictly necessary' cookies.[17] However, such circumstances should be provided by law or permitted by an independent authority, rather than being left to the service provider to decide

[17] https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/

on its own. Our research has shown that it would be a sensible to distinguish a range of uses of tracking devices, and treat them differently depending on the risks involved:[18]

- Strictly necessarily cookies (e.g. load balancing): No need for prior consent;
- Analytics and similar cookies (e.g. error detection): No need for prior consent but users can opt out;
- Legitimate cookies (e.g. tracking cookies): Prior consent needed;
- Illegitimate cookies (e.g. cookies designed to facilitate unfair discrimination): Prohibited regardless of consent.

It should be noted that by prior consent, we do not necessarily mean obtaining consent by 'cookie banners'. In fact, we support communicating user preferences through alternative mechanisms, including browser settings, provided that the choice of users is respected in a meaningful way (see our answers to Q2.4.6 and Q2.4.7 below). Also, where policymakers see the need to retain a degree of flexibility in primary legislation, they can empower an independent authority to specify or approve a list of activities permitted for specific sectors (see our answer to Q2.4.5 below).

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

○ Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
◉ **Strongly disagree**

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

Given the potential intrusiveness of cookies and similar tracking devices, there is no reason to remove the consent requirement for all types of cookies. Quite the contrary, as outlined in our answer to Q2.4.3, the government should consider explicitly prohibiting certain activities involving the use of cookies regardless of user consent.

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?

Sector-specific codes of conduct and regulatory guidance can be a helpful way to keep the legislation open and flexible, while providing additional legal certainty to the industry at the same time. Under Article 40, however, the codes are not legally binding on organisations in the sector, and nor do the codes provide additional compliance incentives to organisations adhering to them. The government should consider the regulatory option of empowering an independent authority to approve sectoral codes of conducts, which may permit certain activities as strictly necessary (no prior consent needed) or comparable to analytics cookies (with 'opt-out consent'). Such codes should be voluntary, but where an organisation makes a commitment to adhere to the code (and thus benefits from the cookie exemptions specified in the code), it should be legally bound by the

[18] https://www.elgaronline.com/view/9781839108297.00019.xml

content of the code. Similar arrangements can be made by means of regulatory guidance issued by the independent authority.

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?

Browser settings and similar solutions may serve as an effective mechanism for users to express their preferences in a much less burdensome manner, especially considering how users may experience 'consent fatigue' with 'cookie banners'. However, if not properly designed, browser settings could be exploited as a blank cheque for online service providers, especially if the configurations of the mechanism do not comply with the data protection by default requirement.

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

As part of our research, we have reviewed the lessons learnt from the history of implementing the Do Not Track (DNT) setting by web browsers and website operators, and found that the initiative did not achieve what was expected primarily for a number of reasons:[19]

- There is a significant disagreement on what amounts to tracking activities (see for example the different interpretations of the 'DNT:1' signal by WP29[20] and W3C[21]);
- The signal is not legally backed by legislation;
- 'DNT:1' signal and similar browser settings can be overridden by more specific consent obtained through, for example, cookie banners;
- There is little commercial incentive for US-based browser manufacturers to invest in the initiative;
- The diversity in browser brands and versions makes it hard to determine whether the signal was transmitted from a compliant browser.

As mentioned, DNT and similar solutions have the promise of simplifying preference communications for users, and hence reducing the overuse of cookie banners, provided that the challenges outlined above are addressed. The present legal reform marks an opportunity for the government to revisit the pledge in 2011 to 'continue to work with browser manufacturers to see if browsers can be enhanced to meet the requirements of the revised [ePrivacy] Directive'.[22] Among other things, the government should especially consider the follow matters:

- How to create commercial and legal incentives for browser manufacturers to develop sector-wide technical standards;

[19] See Chen J, Regulating Online Behavioural Advertising Through Data Protection Law, pp. 132-134, doi: 10.4337/9781839108303

[20] https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20151001__letter_of_the_art_29_wp_w3c_compliance.pdf

[21] www.w3.org/TR/tracking-compliance/

[22] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/77638/cookies_open_letter.pdf

- How to provide legal certainty (e.g. meaning of analytics cookies or tracking cookies) and compliance incentives (e.g. permitting those cookies without consent or only with 'opt-out consent') through legislation, regulatory guidance and sector-specific codes;
- How to make such user preferences binding and enforceable, either backed by legislation or technical solutions (see the Privacy Badger and Global Privacy Control efforts[23]), which cannot be circumvented with cookie banners.

[23] https://www.eff.org/gpc-privacy-badger