DCMS consultation – Data: a new direction

Response from the General Council of the Bar

About the organisation

The General Council of the Bar represents about 17,000 practising barristers in England and Wales. It is also the official regulator of the Bar profession – the regulatory function is delegated to the Bar Standards Board (BSB).

This response is from the whole organisation, but with responses to some questions being more relevant to the representative side and some to the regulatory side. In particular, the responses to questions in section 1.5 are specifically from the representative side. (Not to say the BSB do not agree with this section, it is just they did not address it.)

Chapter 1 – Reducing barriers to responsible innovation

1.2 Research purposes

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

Strongly agree

Please explain your answer and provide supporting evidence where possible

There seems to be no particular reason not to do this. It seems sensible.

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

Somewhat agree

Please explain your answer and provide supporting evidence where possible.

A definition would be helpful, but it needs to be carefully drafted to ensure it does not allow unethical research.

Q1.2.3 *Is the definition of scientific research currently provided by Recital 159 of the UK GDPR a suitable basis for a statutory definition?*

No

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

The definition provided by Recital 159 is somewhat vague and seems to focus on medical and technological research and not on social or policy research. The definition should be precise enough to prevent unscrupulous organisations from using 'research' as a catch-all to enable unethical uses. It would be better if the definition could include a reference to the ethical standards that should be met.

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

Neither agree or disagree

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

Generally speaking, identifying a lawful basis is not an issue for us, as our researchers are able to rely on the lawful basis of 'public task' for research we carry out.

We did not think paragraph 44 was very clear. Are the government considering both the proposals set out here [in Q1.2.5 and 6], or would they only pursue one or the other?

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?*

Neither agree or disagree

Please explain your answer and provide supporting evidence where possible.

Presumably, if there were a separate lawful ground specifically for carrying out research, that would always be used so, by definition, it would help researchers to select the best lawful ground for processing personal data for research purposes, but that does not necessarily mean one is needed. It might be that more guidance is needed to help researchers select the correct lawful ground for their processing of personal data.

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?*

Somewhat agree

Please explain your answer and provide supporting evidence where possible.

It would benefit researchers to clarify that data subjects should be allowed to give their consent to broader areas of scientific research, but the research must remain ethical. Any such provision should not be used as a way of obtaining blanket permission for any type of future project, especially when special category data is concerned. The wording of EU Regulation 2018/1725 Recital 19 is helpful in this regard: "It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have an opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose."

One example where we would find this useful is:

Bar Council collect data on aspirant barristers who apply for pupillage using a website portal (the Pupillage Gateway). They give permission for Bar Council to use their applicant data to monitor access and progression, and we share (grouped anonymous) reporting with the Education and Training organisations who run the pupillages and in our own published Bar Council annual report. We would like to use the data for further analysis on a wider piece of work around a multivariate analysis of personal characteristics of those who attain pupillage versus those who do not, as part of analysing how intersecting personal characteristics (e.g. race, sex, socioeconomic background, education) interact to equate to application success. We believe this further use of data would be permissible under GDPR, but it would be helpful to have that made explicit.

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

Somewhat disagree

Please explain your answer and provide supporting evidence where possible.

Saying a secondary purpose will always be compatible with the original purpose seems to be a very sweeping statement and gives researchers carte blanche to use the data for purposes far removed from the original purpose. While this might be very helpful for researchers, it is likely to weaken the protections for individuals.

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 where it would require a disproportionate effort to do so?*

Somewhat agree

Please explain your answer and provide supporting evidence where possible.

This would be acceptable as long as the new purpose is reasonably compatible with the original purpose – so may not be acceptable if combined with the proposal at paras 48 and 54. Our example in response to question Q1.2.8 could be illustrative of this issue – it might cause disproportionate effort if we were required to supply further information to the individuals concerned in that case.

1.3 Further processing

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

Somewhat disagree

Please explain your answer and provide supporting evidence where possible.

We have had no experience of this causing confusion.

Q1.3.2 *To what extent do you agree that the government should seek to clarify in the legislative test 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?*

Somewhat disagree

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

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

If there is confusion, this should be dealt with by the ICO issuing guidance, rather than amending the legislation.

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?*

Somewhat disagree

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

- *How you envisage clarifying when further processing can take place*
  by the ICO issuing guidance.

- *How you envisage clarifying the distinction between further processing and new processing*
  by the ICO issuing guidance.

1.4 Legitimate interests

Q1.4.1 *To what extent do you agree with the proposal to create a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test?*

Somewhat agree

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

This would be helpful but the suggested list seems to cover topics that are too broad to work with the balancing test which the government will need to do. It does not seem likely that they could do a balancing test that would cover all the circumstances that might arise.

Q.1.4.2 *To what extent do you agree with the suggested list of activities where the legitimate interests balancing test would not be required?*

Somewhat disagree

The suggested list seems to cover topics that are too broad to work with the balancing test which the government will need to do. It does not seem likely that they could do a balancing test that would cover all the circumstances that might arise.

The following section of this response on AI and Machine Learning is from the Bar Council's representative body and not from the BSB.

1.5 AI and Machine Learning

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

Strongly agree

Please explain your answer and provide supporting evidence where possible.

As specified in the consultation §70 "*Fairness can be defined by multiple parameters, ranging from mathematical or technical requirements that relate to outputs, to social or sociological requirements that relate to a fair process. Expectations and legal requirements on fairness currently vary widely. There is a close nexus between fairness, bias, and discrimination, and for the purpose of this consultation, we are treating anti-discrimination, equality measures and measures to combat bias as within the wider ambit of fairness*".

We agree that the concept of fairness is necessarily broad and context specific. Given that AI may be deployed for a range of different and diverse purposes, we see the high level nature of the concept and the adaptability of it to different contexts as a strength, and not a weakness. We believe that this is required in order to provide just and equitable outcomes (both substantially and procedurally) from the development and use of AI Systems.

The principles governing data processing are set out clearly in article 5 of the UKGDPR, the purpose of which is to seek to achieve fairness in data processing. Fairness is and should remain the underlying principle, even though the requirements imposed by adherence to that principle will necessarily vary, according to the specific context, use, impact and risk factors relating to the AI System in question. As paragraph 1(a) of Article 5 of the UKGDPR makes clear, compliance with the principle of fairness also requires transparency; and to ensure transparency, explainability is required.

We believe that the current legal obligations with regards to fairness are clear and are reasonably adaptable when developing or deploying an AI system, without any need to further dilute the data protection regime presently in place, even for research purposes. As mentioned in the Consultation there is also a great deal of guidance available from regulators, non-regulatory actors (including the Centre of Data Ethics and Innovation (CDEI) and Alan Turning Institute) and international organisations, all of which assist in creating frameworks to implement fairness.

We note the definitions provided in the Consultation at §66 and the "Explanatory Box: Data in an AI lifecycle" but note that there are also significant differences in the levels of the challenges to ensuring fairness in the use of different AI Systems and with the use of different data types:

(a) Raw data: which can be personal and non-personal, as well as special categories of personal data (As defined in the Data Protection Act 2018 (s10) and the GDPR Art.9

(b) Pseudonymised data: which as defined within the UK GDPR as "*the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual*" (UK GDPR Art.4(3b))

(c) Anonymised data: the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified.

Whether the data used is raw, pseudonymised or anonymised can be a significant factor in determining the risks posed by the use of a given AI System, both in relation to the manner of deployment and the possible outcomes thereof. For example when using pseudonymised data, one would need to avoid the pseudonymisation code being reversed engineered and/or decoded. For this reason the risks posed by the use of pseudonymised data are greater than the risks posed by the use of truly anonymised data.

Furthermore, the there may be a greater or lesser acceptability of levels of risk depending upon the use to which the AI system is being put: for example, analysis of purchase patterns in a retail context, as opposed to systems for cancer diagnosis, as opposed to wholly automated decision making (in respect of which safeguards are provided by article 22 of the UKGDPR). These are all factors that should be taken into account.

Further, we have limited our response to Artificial Intelligence and Machine Learning as defined within the Consultation and are not dealing with distributed-ledger technology or use of blockchain, which provide added compliance tension in fulfilling obligations under the present data protection regime (Data Protection Act 2018 and UK GDPR[1] and EU GDPR[2]).

[1] United Kingdom General Data Protection Regulation, Retained Regulation (EU) 2016/679 (UK GDPR) (applicable under UK laws from the end of the Brexit implementation period and largely based on the EU GDPR)

[2] EU's General Data Protection Regulation, Regulation (EU) 2016/679 (EU GDPR) (which was applicable under UK laws until the end of the Brexit implementation period at 11 pm UK time on 31 December 2020 and remains applicable in the EEA)

There are also many different types of AI systems, varying with the type of information being processed and the type of response the AI is expected to produce and the impact it has. There are also different categories of AI system based on the scope and scale at which they work. Different levels of risks may exist between supervised and unsupervised machine learning.

Firstly, not only is the quality of the Input Data pertinent as the data samples used to train and test AI Systems can often be insufficiently representative of the populations from which they are drawing inferences. This creates real possibilities of biased and discriminatory outcomes, because the data being fed into the AI Systems is itself flawed from the start and may contain inherent biases. In this regard, AI Systems are trained upon data which may reflect the existing structures and dynamics of the societies they analyse, with the result that data-driven technologies can reproduce, reinforce, and amplify the patterns of marginalisation, inequality, and discrimination that exist in these societies. Further, as many of the features, metrics, and analytic structures of the models that enable data mining are chosen by their designers, these technologies can potentially replicate their designers' preconceptions and (unconscious) biases too.

In these circumstances, we believe that, in applying the underlying principle of fairness to AI systems, it is necessary to take a risk-based approach such as the AI risk-based approach proposed by the European Commission in its publication '[Proposal for a Regulation laying down harmonised rules on AI']() In the Commission's proposal AI systems are divided into three categories:

(i) *Unacceptable-risk AI systems,* which include: (1) subliminal, manipulative, or exploitative systems that cause harm, (2) real-time, remote biometric identification systems used in public spaces for law enforcement, and (3) all forms of social scoring, such as AI or technology that evaluates an individual's trustworthiness based on social behaviours or predicted personality traits.

(ii) *High-risk AI systems,* which include those that evaluate consumer creditworthiness, assist with recruiting or managing employees, or use biometric identification, as well as others that are less relevant to business organizations. Under the proposed regulation, the European Union would review and potentially update the list of systems included in this category on an annual basis; and

(iii) *Limited- and minimal-risk AI systems,* which include many of the AI applications currently used throughout the business world, such as AI chatbots and AI-powered inventory management.

This risk-based approach can be seen as being consistent with the way in which English common law takes an incremental approach to developing concepts such as fairness or reasonableness, taking into account the whole circumstances, including risk factors, in a given case, though we do believe that it would be helpful to this incremental process in relation to the development and use of AI systems, if there were to be an explicit guidance risk levels similar to that proposed by the Commission.

We also believe that such an approach, whilst desirable in itself, would bring the incidental benefit of facilitating the maintaining of the EU adequacy recognition currently accorded to the UK data protection regime.

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

Somewhat agree

Please explain your answer and provide supporting evidence where possible.

Further to Q1.5.1 above, although the UK GDPR and the Data Protection Act 2018 appear to provide an adequate level of clarity on the legal obligations, there appears to be a gap with regard to knowhow (and compliance with sector-related legislation, regulations and rules) and implementation of the obligations by organisations.

The State of AI in 2020 released by McKinsey and Company in November 2020, shows that many organisations still have a lot of work to do to prepare themselves for compliance risks. Only 48% of organisations reported that they recognised regulatory compliance risks and even fewer (38%) reported actively working to mitigate them. Far smaller proportions of the companies surveyed recognised other glaring risks, such as those around reputation, privacy and fairness.

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.*

As an AI System is merely a technical process tool (not an end in itself) used in a particular sector. Therefore, any assessment of fairness should be dependent upon the **activity** which is being regulated as opposed to merely the technology used. There needs to be a collective joint but harmonised collaboration between the relevant regulators with the Information Commissioner's Office (ICO) (taking lead role in the data protection area) in dealing with the substantive assessment of fairness and compliance with the relevant legal obligations. For example, if a Fintech AI System is being used in the financial sector, the ICO and Financial Conduct Authority (FCA), the Payment Systems Regulator (PSR), the Prudential Regulation Authority (PRA) all may need to be involved, depending on the AI activity/context. Organisations should make sure they comply with their legal obligations relating to the activity and the substantive assessment of fairness may well be overlapping. They would need to comply with the highest level of fairness stipulated be the relevant regulatory bodies which falls within the ambit of the activity in which their AI System is used.

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 agree

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

In principle, further clarity of the proposed '*substantive concept of outcome fairness'* would be required to answer this question in detail. Outcome fairness is the prime objective of any decision making whether it be through the use of an AI System or not.

Unfair outcomes can do direct damage to the wellbeing of individuals and the public welfare. They can also undermine public trust in the responsible use of beneficial AI Systems for society, and they can create harmful inefficiencies by virtue of the dedication of limited public resources to inefficient or even detrimental AI technologies, like the COMPASS AI System.

A general 'substantive concept of outcome fairness' may be less adaptable to deal with the different levels of AI System risks (unacceptable/high/limited/minimal risks) that exist (and/or sector-related impact) and may pose further uncertainty in the development and use of AI. Hence we believe that a better approach is to apply the high-level principle of fairness to the particular facts and circumstances of individual cases, (in the context of the risk-based approach which we suggest above) and to allow that high-level concept to develop incrementally.

Further, it may be difficult to fully prove the 'outcome fairness' to a particular required standard; many machine learning AI Systems generate their results by operating on high dimensional correlations that are beyond the interpretive capabilities of human scale reasoning. In these cases, the rationale of algorithmically produced outcomes which directly affect persons who are the subjects of those outcomes, will remain opaque to those subjects. In these AI Systems alternative methods of proving outcome fairness through counterfactual explanations may well be appropriate depending on the circumstances. While in some minimal risk AI Systems, this lack of explainability may be acceptable, in some applications, where the processed data could harbour traces of discrimination, bias, inequity, or unfairness, or where the decisions made could have immense, even life-changing, importance to those affected, the opaqueness of the AI System may be deeply problematic.

We consider the risk-based approach by principles adopted by the EU's proposed AI Act as aforementioned in Q1.5.1 to be a fair way to deal with outcome fairness, allowing flexibility to deal with the innovation of AI Systems in the different sectors as well as well as dealing with the near/medium-term future advances in the use of AI Systems.

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

Strongly disagree

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

The present data protection regime (under the Data Protection Act 2018 and GDPR regimes) provides baseline safeguards uphold societal values and to protect the fundamental rights of individuals. These safeguards should not be diluted in order to support AI developers in the training and testing of AI Systems. AI development and implementation should respect those safeguards in order to maintain public confidence and trustworthiness. The importance of the fundamental rights of data subjects, including the right to privacy and the UKGDPR rights to fairness (as it relates to discrimination, bias, transparency, accountability), should override the need to change the landscape in favour relaxing the practical compliance requirements of AI developers. Threats to privacy are posed by AI systems as a result of their design and development processes, and as a result of their implementation. The personal data used by AI Systems is sometimes captured and extracted without gaining the proper consent of the data subject and/or without the data subject's knowledge, or is handled in a way that reveals (or places under risk the revelation of) personal data, even including special category data. In consequence, without adequate safeguards, there may well be unfair devastating consequences to the individual.

In these circumstances, whilst we see the desirability and importance of training and testing of AI, especially so as to ensure that it is itself fair and free of bias, nonetheless, this must not be at the cost of proper compliance with data protection obligations. This is not, we believe, an onerous responsibility. For example, it may be that that developers could consider using anonymised data rather than pseudonymised or raw data as a means of ensuring privacy compliance. Pseudonymisation and anonymisation are techniques that can in some circumstances be used either (i) as a security measure, to minimise the risk to data subjects and help the controller to meet its legal data protection obligations or (ii) (in the case of anonymisation, to remove information from the scope of the data protection regime.

Q1.5.6 – Q1.5.9

The Bar Council is not engaged in developing AI systems and has no experience in this area.

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

Strongly disagree

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

○ *the key benefits or risks you envisage*

○ *what you envisage the parameters of the processing activity should be*

Whilst we can see some utility in the creation of a non-exhaustive list of possible legitimate interests justifying the processing of data (for example in relation to “legitimate interest” under article 6(1)(f) of the UKGDPR) as a means of giving additional guidance to data processors as to the sort of things which might constitute a legitimate interest, we strongly disagree with the proposal to set out an exhaustive list of specific “legitimate interests” in respect of which no balancing against fundamental rights would be required.

We have set out above, and here affirm our belief that the safeguards in relation to fundamental rights should be neither abrogated nor diluted.

Of course, we should have no issue with a 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 provided however that the balancing requirement is also maintained.

The proposals under §91 of the Consultation are most likely to result in a disproportionate increase of processing of personal data of individuals with protected characteristics, and therefore cause a greater likelihood of intrusion into their private and family lives, and cause a greater risk of a breach involving their personal data. We do not consider the adverse effect likely to be suffered by individuals with protected characteristics to be objectively justifiable in all circumstances hence why a balancing test should be required. More guidance (from for example the CDEI or the ICO) on the application of the Equality Act to AI Systems decision may be of assistance to organisations.

Our fundamental concern, however, is that, even under the existing law, developers may be all too eager to believe (albeit wrongly) that legitimate interest trumps privacy rights, and that it may be used as a justification for processing special category data[3] : it would be unfortunate if such intrusions on fundamental rights were now to be given even limited legal sanction.

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 disagree

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

We strongly agree that further legal clarity is needed on how sensitive personal data may be lawfully processed for the purpose of ensuring bias monitoring, detection and correction in relation to AI systems.

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 disagree

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

We would strongly disagree with this proposal for the reasons which we have clearly articulated above. We would support the continuance of the requirement under article 9 of the UKGDPR for actual consent for the processing of special category personal data. It does require to be borne in mind that, under the UKGDPR, fully anonymised data loses its quality of being personal data, and, hence, may be used for the purposes suggested. The proposal appears to envisage the use of special category personal data without anonymisation. We can see no justification for such a provision, even to support the processing of sensitive

[3] In this regard see this recent Whistleblowing case: https://www.gov.uk/employment-tribunal-decisions/mr-c-costagliola-di-fiore-and-ms-h-s-qadri-v-introhive-uk-ltd-2203125-slash-2020-and-2203126-slash-2020]

personal data for the purpose of bias monitoring, detection and correction in relation to AI systems.

The idea of a new condition within Schedule 1 to the Data Protection Act 2018 which specifically addresses the processing of sensitive personal data as necessary for bias monitoring, detection and correction in relation to AI systems without any consent by the data subject does not appear to be justified. If data is fully and effectively anonymised, it ceases to be personal data. However, the process of anonymisation does involve the processing of personal data, and it may be appropriate to make it clear that this limited processing would be permissible.

Subject to that minor qualification, the safeguarding parameters mentioned in §91(b) of the Consultation, being:

(i) *ensuring the processing is strictly necessary for this purpose;*

(ii) *data is explicitly collected for bias/discrimination mitigation and not for any other purpose; and*

(iii) *appropriate safeguards to remove risks of secondary use, e.g. by specifying technical limitations on re-use, and the implementation of appropriate security and privacy preserving measures."*

would be insufficient to justify the intrusion of privacy, potential risks and adverse impact to the relevant data subjects and detrimental effects likely to be encountered.

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

This depends on the context of the conditions imposed and whether the data subjects' rights are adequately protected. Anonymisation of data and/or compliance with Article 9 of the UK GDPR would be required.

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

Article 22 UK GDPR only applies to decisions based solely on automated decision making, including profiling, without any meaningful human intervention that has a legal or similarly significant effect. We can see that there may be some scope for additional guidance in this regard.

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

○ *The benefits and risks of clarifying the limits and scope of 'solely automated processing'*

Automated decision-making can be either:

(i) solely automated decision-making, where the AI system makes the decision automatically, or

(ii) partly automated decision-making (decision support), where the AI system only supports a human decision maker in their deliberation

These are treated differently under the data protection regime, as only solely automated decisions are subject to Article 22 UK GDPR. However, the degree and quality of human review and intervention in the decision-making process are key to determining whether an AI system is being used for automated decision-making or as decision support. If it the level of human input or review is insufficient then seemingly partial automated decision-making may, in fact, be solely automated decision-making.

There is usually a concern or, sometimes, confusion as to what activity would qualify as human intervention. In order for an activity to qualify as 'human intervention', the intervention has to be meaningful. It must be carried out by an individual who has the authority and competence to change the automated decision and to do so considering all the available input and output data. In other words, the intervention cannot simply be a token gesture—there must be the ability for human review of the decision, along with discretion to alter it before it is applied. If human involvement is limited to applying a decision made automatically without any real discretion to change it, then the decision is based solely on automated processing. This may cause ambiguity particularly:

(i) where the risk of automation bias or automation complacency needs to be considered, where the human reviewer stops using their own judgment because they perceive the automation to be more trustworthy; or

(ii) where a lack of explainability and consequent interpretability of the decision by complex machine learning AI Systems make it difficult for a human reviewer to meaningfully assess the output of the AI System and leads the reviewer with little option but to accept the recommendations without judgment or challenge.

Clarification that the level of human involvement should not be superficial or substantially biased by the output of the algorithm, or that the human's judgment should not be affected by other conscious or unconscious biases, would be very useful.

Further, the level of information that would be required to be given to data subjects when exercising their rights under article 22 or other similar transparency provisions may cause concerns for AI developers and users relying particularly on fully automated-decision making AI Systems. These concerns arise from not only from the difficulty in providing a comprehensible justification for the decision or review, but also possible requirements to protect trade secrets or the rights of other data subjects.

Additionally, clarity on automated decision making with regard to children would be useful to supplement the ICO guidance which merely states that in 'most circumstances' these should not be made in respect of children.

Data processing under Article 22 is inherently a process which poses high risks and, indeed, is recognised as a high rsk process under the Commission proposals. Therefore, a DPIA must be carried out alongside the use of other safeguards. Recital 71 of each of the GDPR further highlights that, in any type of processing under Article 22, suitable safeguards should include provision of specific information, the right to obtain an explanation of the decision reached and the right to challenge that decision. Clarification of what is meant by the right to obtain an explanation could be usefully be given, so as to extend this right to a right to be informed and provided with a valid justification as opposed to, or in addition to, simply a the right to an detailed explanation of how, technically, the AI System has made the decision.

○ *The benefits and risks of clarifying the limits and scope of 'similarly significant effects'*

The terms '*legal effect'* or '*similarly significant'* are not defined in the UKGDPR However, the Working Party guidance states that the wording in the GDPR makes it clear that only serious effects are covered by Article 22 of the GDPR. A decision has a similarly significant effect where it has an impact upon a person's circumstances, behaviour or choices that is equivalent to a decision producing a legal effect. In other words, even where no legal (statutory or contractual) rights or obligations are specifically affected, a data subject could still be impacted sufficiently to require the protections under this provision. This allows leeway for misunderstandings to be created on the interpretation of '*serious effect'* or '*similarly significant'*. As stated in the Consultation, organisations may mistakenly assume that Article 22 does not apply to them or their processing activities, potentially leading to loss of the safeguards where they are needed, or reverting to a risk-adverse approach as a default, and resulting in not using fully automated decisions at all, even where it may have been acceptable to use such decision making systems.

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

No

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

There does not appear to be any evidence of a problem here nor any need for alternatives to the current data protection regime as it stands, save for better guidance and/or clarifications as expressed under our answers to Q1.5.13 and Q1.5.14.

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

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

Looking at the likely short and medium term development of AI Systems (which for some time are likely to remain as narrow/weak AI systems) we do not believe that further change in the data protection regime is, in this regard, required at present. However, circumstances may change and develop over time and we welcome the Government's seeking of evidence to reconsider whether there is any need to be addressed.

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

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

○ *The benefits and risks of the Taskforce's proposal to remove Article 22 and permit solely automated decision making where (i) it meets a lawful ground in Article 6(1) (and, Articles 9 and 10, as supplemented by Schedule 1 to the Data Protection Act 2018) in relation to sensitive personal data, where relevant) and subject to compliance with the rest of the data protection legislation.*

The safeguards under Article 22 of the UK GDPR are meaningful and meant to protect data subjects against the risk that a potentially damaging decision is taken in relation to them without any human interventions by an automated decision-making process. We would strongly disagree 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, as there is a basic legitimate expectation in society, that some form of human intervention should take place in respect of decisions with legal effects for the individual.

The removal of such a protection is likely to be counter-productive, reducing public confidence and acceptance of AI as a decision-making or decision-aiding tool and thereby hampering the legitimate development and use of AI systems.

○ *Any additional safeguards that should be in place for solely automated processing of personal data, given that removal of Article 22 would remove the safeguards currently listed in Article 22 (3) and (4)*

Considering that we disagree with the removal of Article 22 of the UK GDPR as aforementioned this question does not apply. Public trust in the use of data-driven systems is critical if the full benefits of properly regulated AI are to be unlocked.

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.*

Profiling and automated decision-making are used in a number of sectors, both private and public. Advances in technology and the capabilities of big data analytics, artificial intelligence and machine learning have made it easier to create profiles and make automated decisions with the potential to significantly impact individuals' rights and freedoms. While both can be useful tools for individuals, organisations and the economy in general, they can also pose significant risks to individuals' rights and freedoms which require appropriate safeguards.

We should be strongly supportive of any proposals to increase public trust and confidence in the use and development of AI Systems by protecting human rights and using AI Systems to provide fair and just outcomes.

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

We mention above in our answers to Q 1.5.13 and Q1.5.14 the clarifications which might be made. We also refer to the need to maintain the safeguards afforded by Article 22 of the UKGDPR.

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.*

We have no strong views in this matter, beyond our support for data protection as an essential component in addressing such potential harms as might be identified.

Chapter 2 – Reducing burdens on businesses and delivering better outcomes for people

2.2 Privacy management programmes

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

Somewhat disagree

Please explain your answer and provide supporting evidence where possible.

One way of looking at this is that having a 'more flexible', 'less prescriptive' system means that it is going to be more difficult than it is at present to know when your systems comply with the legislation. There are a lot of references in this consultation to a lack of clarity making it difficult for organisations – is this proposal just going to add to that lack of clarity? Also, how will it affect organisations that also operate in Europe? They will have to follow two separate regimes, not just one – adding to their burdens, rather than reducing them.

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

Somewhat 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.*

Yes, this proposal is very likely to create additional burdens on organisations. While organisations may not currently have a 'privacy management programme' as such in place, many will already have in place many elements that one would require. While these proposals are suggesting getting rid of some of the current requirements, such as

DPIAs, because they are too prescriptive, there is still a requirement to 'adopt different approaches to identify and minimise data protection risks'. So how is getting rid of DPIAs helping, leaving organisations to formulate their own risk assessments? If the government is to deliver on its promise that 'the protection of people's personal data must be at the heart of our new regime' then how is taking away some of the prescriptive elements of the current regime going to help unless it is intended that the current safeguards are watered down? And this particular proposal, while possibly watering down the safeguards, is actually increasing the work involved by needing organisations to come up with alternative approaches.

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

Somewhat disagree

Please explain your choice and provide supporting evident where possible.

For individuals to benefit from this change, it would have to mean that safeguards on people's data would be improved by developing privacy management programmes. This seems unlikely if the PMPs end up watering down the current safeguards. Any improvements that might be made could, most probably, be achieved by more minor changes to the current accountability requirements. Given that PMPs would be in place to ensure data is kept secure etc, data subjects are only going to 'benefit' if the programme prevents a data breach or similar detrimental effect on the data subject. It is difficult to quantify such benefits.

- *Please share your views on which, if any, elements of a privacy management programme should be published in order to aid transparency.*
  How to request information and make complaints and how these will be handled (organisations should be doing this already, though).
- *What incentives or sanctions, if any, you consider would be necessary to ensure that privacy management programmes work effectively in practice.*

  The ICO would need to publish guidance on what a PMP should look like in order to satisfy the ICO it would work effectively in practice. The ICO would also need enforcement powers to deal with cases where organisations do not have effective PMPs, particularly if they experience data breaches.

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'?*

Somewhat agree

Please explain your choice and provide supporting evident where possible.

The suggestion that organisations are not able to appoint suitably skilled DPOs because of a skills shortage should not be addressed by taking away the requirement for organisations to have a DPO, is specific circumstances.

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

Please explain your choice and provide supporting evident where possible.

It may be sensible to remove the requirement for all public sector bodies to designate a DPO and apply the same criteria to public bodies as are applied to private organisations for designating a DPO. This is because some public bodies are small and/or may not process much personal data. However, we do not agree with the sentiment in para 162 about some organisations struggling to appoint suitable individuals who are sufficiently independent from other duties. If it is an issue to have a dedicated DPO in a smaller organisation, then an external consultant DPO could be appointed instead, or a number of smaller organisations could share a DPO. The current requirement for a DPO to have an independent role in an organisation is important to ensure data subjects' rights are properly addressed. This would be lost by replacing the DPO with a 'responsible individual' as set out in the proposals for PMPs.

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

Some organisations had data protection officers before the introduction of GDPR, and many more have appointed or designated them since. Given that, even if all the proposals become law, there is still a significant role to ensure data protection compliance, many organisations are likely to leave things as they are and keep their DPO role. However, they would still need to appoint the 'responsible individual' as set out in the PMP proposals, thus increasing the burden on some organisations.

Data protection impact assessments

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

Please explain your choice and provide supporting evident where possible.

It has taken some time to become familiar with the requirements of DPIAs and become accustomed to carrying them out. But, having done so, we now find them an invaluable tool in helping to identify and mitigate risks arising from new processing. We have had experience of how things can go wrong when a DPIA is not done at the appropriate time – especially where contractors are involved. We have discovered that, while DPIAs take a little time and effort, they are worthwhile, and definitely not a box-ticking exercise.

Q2.2.8 *To what extent do you agree with the proposal to remove the requirement for organisations to undertake DPIAs?*

Strongly disagree

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

The proposed privacy management programmes require ‘risk assessment tools for the identification, assessment and mitigation of privacy risks across the organisation.’ It is therefore unclear how removing the requirement to do DPIAs has any impact on reducing the burden on businesses. DPIAs are only mandatory in certain circumstances under the current legislation. Presumably then, in those circumstances a risk assessment would still be required under the new proposal. DPIAs are a risk assessment tool, which we have embedded into our processes and trained staff on. Why should we have to formulate our own methods, when the DPIA process exists already? Having guidance provided by the ICO on when DPIAs are needed and how to carry out a DPIA is much more straightforward than a blank sheet of paper. The fact that considering DPIA is mandatory is helpful from a compliance point of view, in that it is an aid to getting co-operation from colleagues to get the DPIA done.

The only way removing the need to carry out DPIAs is going to reduce the burden is if fewer risk assessments are done. Having had experience in our organisation of how things can go wrong when a DPIA is not carried out – the work involved in putting things right can be a much bigger burden than doing the DPIA in the first place.

Prior consultation requirements

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

Please explain your answer and provide supporting evidence where possible.

Presumably because where such a situation arises, the organisation decides not to proceed with the processing rather than go through the process of consulting the ICO only to have them recommend against the processing. If this requirement was taken away, however, organisations may be more likely to risk proceeding with the high risk processing.

Record keeping

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

Somewhat agree

Please explain your answer and provide supporting evidence where possible.

The Record of Processing Activities (RoPA) is quite a burden to draw up and maintain and it is not widely referred to in our organisation. It is also very unwieldy because there is so much information in one spreadsheet (or whatever format of document). Perhaps the requirement could be to have a record of the various elements set out in Art 30, but not all in the same document, and not with each element recorded against every bit of processing but recorded in a more general way, eg on security of systems.

Breach reporting requirements

Q2.2.12 *To what extent do you agree with the proposal to reduce burdens on organisations by adjusting the threshold for notifying personal data breaches to the ICO under Article 33?*

Somewhat disagree

People are always going to report data breaches even when they do not reach the threshold for reporting 'just to be on the safe side'.

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?* No. The proposed change in wording is not a significant change and is unlikely to have a major impact on the number of reports. It is not clear what is meant by 'material'. It would be better to provide a more clearly worded threshold (without including a 'double negative') and to give some clear way of assessing if a breach meets the threshold or not – perhaps by some sort of scoring system. Generally, the situation might be best resolved by the ICO issuing better guidance on reporting than changing the wording of the legislation.
- *Would the adjustment reduce burdens on organisations?* Unlikely. The burden is investigating the breach incident, deciding if it is a breach and, if so, how to mitigate in this instance and to prevent future similar incidents, and if data subjects need to be contacted. This is needed whether a breach ends up being reported to the ICO or not. The actual reporting is not particularly burdensome, although an ICO investigate possibly is. But if a report is made when it was not needed, the ICO will not investigate in any case. The only way this would reduce the burden is if, by increasing the threshold, the ICO investigate fewer breaches.
- *What impact would adjusting the threshold for breach reporting under Article 33 have on the rights and freedoms of data subjects?* Not a great impact. As long as breaches are still reported that meet the current higher threshold that requires organisations to notify data subjects as well, there is unlikely to be much difference to data subjects. But if, by increasing the threshold the ICO do not investigate a breach that they would have done before the threshold was changed, this results in an issue not being picked up, this may later cause a more significant breach which does detrimentally affect data subjects.

Voluntary undertakings process

Q2.2.13 *To what extent do you agree with the proposal to introduce a voluntary undertakings process? As a reminder, in event of infringement, accountable organisations allowed to provide the ICO with remedial action plan which, if it met certain criteria, ICO could authorise without taking any further action.*

Somewhat disagree

Please explain your answer and provide supporting evidence where possible

Seems like a way for an organisation to try and hide the full extent of an infringement and prevent the ICO from investigating.

If the govt chooses not to pursue the implementation of privacy management programmes, certain elements of this proposal could be implemented as stand-alone reforms. It welcomes views on the following questions, relating to alternative reform proposals should privacy management programmes not be introduced:

Record keeping

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

Somewhat agree

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.

Some elements are duplicative, but the Record of Processing Activities (RoPA) goes into much greater detail compared to privacy notices, for example. It provides (or should provide) a record of all an organisation's processing activity in one place, whereas Art 13 and 14 data may be provided in many separate locations. Having said that, the RoPA is not greatly used. There is overlap with retention schedules too.

Article 30 (1)(a) and (f) are duplicated. (1)(g) also seems unnecessary to record for each piece of data listed on the RoPA as it will be the same for large sections of the data listed, if not all of it.

Breach reporting requirements

Q2.2.17 *To what extent do you agree with the proposal to amend the reporting requirement could be implemented without the implementation of the privacy management programme?*

Somewhat agree

The proposal could be implemented but, as it stands, we do not agree that it should be.

Further Questions

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 on record keeping, breach reporting requirements and data protection officers?*

None.

The following section of this response on Subject Access Requests is more relevant to the regulatory body, the BSB, than the representative body of the Bar Council, as the BSB receive the vast majority of the SARs received by the organisation.

2.3 Subject Access Requests

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

Please provide supporting evidence where possible, including:

- *What characteristics of the subject access requests might generate or elevate costs?* The fact that we hold a large volume of personal data on certain individuals and their tendency to request everything when they make SARs. We often also need to carry out a good deal of redaction, to remove legally privileged material and the personal data of other people (which can often be special category data).

  In the last two years a significant proportion of requests we have dealt with required outsourcing some of the work. These amounted to 8 out of a total of 18 were outsources in 2019/20 and 7 out of 21 in 2020/21. The Bar Standards Board lacks the internal capacity to process very large SARs as the organisation is too small to have a dedicated team to handle requests. Nonetheless, there was still internal work required on providing instructions, reviewing and preparing the response and corresponding with requesters.

  Examples of the high costs are that in 2019/20 four out of eight SARs we outsourced cost more than £1,500. In 2020/21, three out of six SARs outsources cost more than £1,500. The remainder cost £1,000 or less.

- *Whether vexatious subject access requests and/or repeat subject access requests from the same requester play a role*
  We do receive repeat requests from certain individuals which definitely plays a role in elevating costs. Vexatiousness is not a particular issue for us other than that some requests do cause ‘disruption’ but perhaps not that the requester intended this. Adding criteria for ‘vexatiousness’ might be helpful.

- *Whether it is clear what kind of information does and does not fall within scope when responding to a subject access request.*
  We do seek clarification from requesters sometimes, but this is often in an effort to cut down the volume of material we need to go through. We will, for example, ask them to give us a time period that they are interested in, or specific parts of the organisation they have communicated with. This is sometimes successful, but on other occasions they will still insist on receiving all their data. We just find some requests very excessive and believe the requesters are making speculative requests with a view to litigation.

Q2.3.2 *To what extent do you agree with the following statement: ‘The “manifestly unfounded” threshold to refuse a subject access request is too high’?*

Strongly agree

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

We do believe that SARs are sometimes used as a means of circumventing strict disclosure protocols under the Civil Procedural Rules. Part of the function of the Bar Standards Board (BSB) is to investigate reports of inappropriate behaviour by barristers. These investigations can result in sanctions against barristers, the most serious of which is that they are disbarred. Barristers being investigated will often submit a SAR to the BSB. The ability to consider the purpose of the request would be helpful in these circumstances, especially if we could then consider such requests 'manifestly unfounded'. It would be helpful if providing the purpose for requesting the information was made mandatory and the organisation is only obliged to provide data relevant to that purpose. Currently, we believe SARs present a disproportionate cost to our organisation relative to the benefit to requesters.

Q2.3.3 *To what extent do you agree that introducing a cost limit and amending the threshold for response, akin to the FOI regime would help alleviate potential costs (time and resource) in responding to these requests?*

Somewhat agree

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

- *Which safeguards apply (such as mirroring Section 16 of the FOIA (for public bodies) to help data subjects by providing advice and assistance to avoid discrimination)*

  If we were able to apply a cost limit as under FOIA this might help limit the scope of the request to something more manageable. The requester should still be able to get the information they really need. We would be happy to provide advice and assistance to facilitate that, but a requirement on the part of the requester to tell us the purpose of the request would most likely be needed for us to be able to do this.

- *What a reasonable cost limit would look like, and whether a different (ie. sliding scale) threshold depending on the size (based on number of employees and/or turnover, for example) would be advantageous*

  A cost limit of £450-600 (as with the current FOIA regime) would have a significant benefit for us. Time recording carried out by staff between August – October 2021 shows that typically SARs which are not excessive cost in the region of £75 - £500.

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 DPA 1998)'?*

Strongly disagree

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

Re-introducing the nominal fee would have no impact on barristers but could potentially be prohibitive for members of the public. A fee could be discriminatory against those with limited resources even if it is 'small'. In the year 2019/20, of the 18 SARs received by the Bar Standards Board, 12 were from barristers and 6 were from members of the public. In 2020/21, 21 SARs were received, 15 from barristers and 6 from members of the public. Therefore, introducing this requirement would have a limited impact on the volume, size and thus organisational burden of responding to requests.

The previous fee of £10 made no impact on the cost to an organisation of dealing with SARs, as in some cases, it would cost an organisation more to process the fee than the fee itself. So it would be purely a deterrent. In our organisation, under the previous data protection regime we waived the £10 fee in any event for vulnerable requesters or those of limited means. If the government means it when it says 'The protection of people's personal data must be at the heart of our new regime' and 'These reforms will keep people's data safe and secure…', then the reintroduction of a fee for SARs does not seem to fit, given the reason for making a SAR is supposed to be to allow the data subject to 'be aware of, and verify, the lawfulness of the processing' of personal data. While it would be helpful to limit data subjects' ability to make SARs to this stated purpose, the reintroduction of a fee is not the way to achieve that.

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

Yes

Please explain your answer and provide supporting evidence where possible.

A rule which would allow organisations not to have to provide data that they have sent to the requester before (in the normal course of business rather than in response to a previous SAR), or to allow them to charge for providing such data.

2.4 Privacy and electronic communications

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

Somewhat agree

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

It would improve the accuracy of the data obtained for website analytics if consent was not needed for analytics cookies, so we are in favour of the proposal.

The 'soft opt-in' in relation to direct marketing activities

Q2.4.9 *To what extent do you agree that the soft opt-in should be extended to non-commercial organisations? (see para 208 for description of 'soft opt-in')*

Strongly agree

Please explain your answer and provide supporting evidence where possible.

We would see this as a useful change. While we get consent from barristers for most of the communications we have with them, there are some situations where it would be useful to communicate on a matter where we have not collected prior consent. For example, BSB send a Regulatory Update email to all practising barristers but do not have consent from unregistered barristers to also send it to them (where we have email addresses for them). The 'soft opt-in' might enable BSB to also send the Regulatory update to those barristers as well. In addition, there might be other groups, such as students, where we establish a relationship with them when they sit an exam run by BSB, and the soft opt-in would enable us to communicate with them about events we are running, for example.

Chapter 3 – Boosting trade and reducing barriers to data flows

Derogations

Q3.5.1 *To what extent do you agree that the proposal described in para 270 represents a proportionate increase in flexibility that will benefit UK organisations without unduly undermining data protection standards?*

Somewhat agree

Please explain your answer and provide supporting evidence where possible.

This change could be useful to organisations like ours. Often, our international transfers of personal data only arise because we are using a data processor (generally some sort of IT provider) which involves sorting data outside the EEA. Often, this situation is dealt with by SCCs, but there have been occasions where these have not been available to use and consent or performance of a contract has had to be used instead. Companies that provide such services are often US-based and have been affected by the loss of the Privacy Shield. For example, using a US-based online exam platform which was relying on the Privacy Shield when Schrems II happened, and the Shield was invalidated overnight.

Chapter 5 – Reform of the ICO

5.3 Governance Model and Leadership

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

Strongly disagree

Please explain your answer and provide supporting evidence where possible

This would threaten the independence of the office of the ICO.

5.4 Accountability and Transparency

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?*

Somewhat agree

Please explain your answer and provide supporting evidence where possible

A regulator publishing key strategies and processes would be welcomed, in the interests of openness and transparency.

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

Somewhat agree

Please explain your answer and provide supporting evidence where possible

We agree with this proposal, if a suitable threshold was set.

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 govt may initiate an independent review.*

Not meeting the key performance indicators by a significant margin.

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

Please explain your answer and provide supporting evidence where possible

This proposal does not seem unreasonable where the impact of a code of practice or new guidance could be substantial.

Q5.5.2 *To what extent do you agree with the proposal to give the Sec of State the power to require the ICO to set up a panel of persons with expertise when developing codes of practice and complex or novel guidance?*

Somewhat agree

Please explain your answer and provide supporting evidence where possible

This proposal would help to ensure codes of practice and guidance are entirely appropriate, especially in fields where the ICO may not have all the relevant expertise in-house.

Q5.5.3 *To what extent do you agree with the proposal to give the Sec of State a parallel provision that afforded to the Houses of Parliament in Section 125(3) of the DPA 2018 in the approval of codes of practice, and complex and novel guidance?*

Strongly disagree

Please explain your answer and provide supporting evidence where possible

This is a threat to the independence of the office of the Information Commissioner. We agree with the ICO's own assessment that it would reduce the ability of government to hold the ICO accountable and would reduce clarity over whose guidance it is – the ICO's or the government's? Given the ICO is there to regulate the government for FOI and data protection, this seems particularly inappropriate.

5.6 Complaints

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 agree

Please explain your answer and provide supporting evidence where possible

It makes sense to give the organisation concerned an opportunity to resolve a complaint before it goes to the ICO. This is also in line with other complaints and Ombudsmen organisations where introducing this requirement has worked well. It should reduce the workload of the ICO, allowing them to concentrate their efforts of the more serious matters, and enable complainants to get a faster resolution in many cases.

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

Strongly agree

Please explain your answer and provide supporting evidence where possible

For the proposal at Q5.6.2 to work effectively, the proposal for data controllers to have a complaints procedure is essential. Otherwise, the requirement to make complainants go to the data controller first could just add an additional step and waste time in getting their issue resolved.

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

This should be mandatory for all but very small private businesses.