IRSG
INTERNATIONAL
REGULATORY
STRATEGY GROUP

**IRSG RESPONSE TO 'DATA: A NEW DIRECTION'**

*The International Regulatory Strategy Group's response to the Department for Digital, Culture, Media and Sport's consultation on the future of the UK's data protection system.*

The International Regulatory Strategy Group (**IRSG**) is a practitioner-led body of leading UK-based representatives from the financial and professional services industry. It is an advisory body to the City of London Corporation, and to TheCityUK. The IRSG develops its policy positions through a number of workstreams which comprise representatives from across the financial services industry to ensure a cross-sectoral response.

We thank you for considering this submission.

For any questions or clarifications please contact: IRSGsecretariat@cityoflondon.gov.uk.

CONTENTS

**INTRODUCTION**

Our members welcome the opportunity to respond to this Consultation Paper (CP) on the UK's future legislative and regulatory data regime. The government has proposed a range of reforms, which are wide-ranging and complex. The points set out in this response represent the consensus among our members.

We wish to make the following general observations:

1. We recognise and support the government's intention to create a "pro-growth and pro-innovation data regime whilst maintaining the UK's world-leading data protection standards." Whilst we agree that there are targeted opportunities to streamline and optimise the current regime, it is important to acknowledge that implementation of the existing regime has been largely successful and that removing its features 'in bulk' might cause uncertainty for both data subjects and businesses.

2. Our members do not wish to see increased compliance costs, especially since the government takes the view that organisations currently complying with the UK GDPR and the Data Protection Act 2018 ("**DPA**") regime are likely to be compliant with the proposed new framework.

3. We welcome the stated policy objective of increasing digital trade with other countries and agree that expanding the number of adequacy decisions will support this objective. At the same time, our members would like to emphasise the importance of ensuring such expansion takes into consideration both: (i) the ongoing robust protection of personal data; and (ii) the importance of maintaining the current EU adequacy decision. Many of our members have emphasised the risks associated with the introduction of obstacles to the free flow of data between the UK and EU.

4. Our members consider that the continued independence of the ICO is paramount. Regardless of how the government structures the statutory framework for the ICO, as a matter of good regulation and good principle (and to avoid endangering the EU adequacy decision), it should maintain the independence of the ICO.

5. While we have answered each question individually, our answers should be read as a whole setting out the totality of protection standards that we consider appropriate.

## CHP 1 - REDUCING BARRIERS TO RESPONSIBLE INNOVATION

### 1.2 Research purposes

***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**
We welcome the creation of a statutory definition of "scientific research" as it will provide greater certainty for organisations.

***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**
We recognise that Recital 159 serves as a good starting point for a statutory definition.

To encourage businesses to carry out responsible innovation, we recommend expanding and clarifying any statutory definition to include research carried out by a business for the purposes of developing new products and services and research conducted with a view to assessing and improving Environmental, Social, and Governance ("**ESG**") and Diversity, Equity, and Inclusion ("**DE&I**") outcomes.

***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 disagree**
We consider it good discipline and best compliance practice to require the identification of a lawful basis of processing. We do not consider this creates a material barrier to research.

### 1.3 Further processing

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

**Somewhat agree**
We agree that the test within Article 6(4) of the UK GDPR can be challenging and complex to apply in practice. We would welcome additional clarity from the government on the compatibility of further processing, in particular on the internal use of data previously collected by businesses for developing new products and services.

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

**Strongly agree**
We support the proposal.

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

**Strongly agree**
We support the proposal.

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

**Strongly agree**
We support the proposal.

**1.4 Legitimate interest**

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

**Strongly agree**
We agree that creating a list of processing activities on which organisations may rely without applying a balancing test would be in the interests of both organisations and individuals. Specifically, it would provide much-needed certainty when relying on legitimate interests as a lawful basis of processing and would remove unnecessary compliance costs.

However, two points should be noted:

- It should be made clear that processing activities that may benefit from reliance on legitimate interests (after conducting a balancing test) are wider than this list.
- Clarity should be provided as to whether falling within the scope of one of these pre-defined legitimate interests categories would constitute either *prima facie* evidence, or a rebuttable presumption, of "compelling legitimate grounds" for the purposes of Article 21(1) of the UK GDPR.

***Q1.4.2. To what extent do you agree with the suggested list of activities where the legitimate interests balancing test would not be required?***

**Somewhat agree**

We agree with the suggested list of activities where the legitimate interests balancing test would not be required. We particularly welcome the proposal at 'h' which we consider will foster a better environment for innovation.

We propose the list be expanded to include the following additional processing activities:

- Processing necessary for the purposes of litigation, arbitration, internal or external investigations;
- Processing linked to reliance on conditions within Parts 1, 2 or 3 of Schedule 1 to the DPA, where we consider the need to undertake additional steps to demonstrate compliance pursuant to Article 6 of the UK GDPR is unnecessary;
- The retention of payment card data to facilitate future payments (without the need for a customer to enter their details with every transaction);
- Supporting the realisation of ESG and DE&I objectives, for example those emanating from COP26;
- Detection, investigation and prevention of economic crime; and
- The processing of personal data for identity verification (this could be included under 'f) improving the safety of a product or service that the organisation provides or delivers').

Our answer to this question should be read together with our responses to other questions to ensure that the totality of the protection provided by the UK data protection regime is deemed adequate. In particular, if the DPIA process is removed, some kind of control serving a broadly equivalent purpose as the balancing test will be needed in relation to the second and fifth bullet points above.

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

We suggest that the government and/or ICO consider a public information campaign, possibly with the use of standardised icons, to advise individuals where processing is based on a regulator-approved list.

Guidance and examples from the regulator around general items such as: h) Using personal data for internal research and development purposes, or business innovation purposes aimed at improving services for customers' and 'f) Improving the safety of a product or service that the organisation provides or delivers' will help provide clarity and certainty both for businesses and consumers on which activities qualify for this list.

**1.5 AI and Machine Learning**

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

**Somewhat disagree**

Although the current framework and legal obligations are rooted in principles based human rights and data protection law, we recognise that when translating for a relatively nascent and technically complex field such as AI, fairness can have different and sometimes incompatible meanings, and therefore, legal obligations to meet compliance requirements.

In our view, while the UK has and continues to set the standard globally with regard to fairness, accountability and transparency requirements for AI systems, this will require a more comprehensive and iterative approach before more easily usable frameworks and a path to demonstrable legal compliance emerges.

***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**
The application of the concept of fairness in AI continues to develop, as it should, and the legal requirements in relation to transparency and discrimination are broadly appropriate.

***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?***

AI should not be treated as somehow *sui generis*. As AI systems are deeply rooted in many other aspects of societal and technological developments historically, and will continue to going forward, we feel it is important that human rights, employment equality and criminal law continue to play an important role in substantive assessments of fairness.

It would be helpful for the ICO to produce guidance on what "fairness" means in the AI context, rather than defining fairness in legislation. We also suggest the approach of regulators developing rules on the detection and mitigation of specific fairness-related harms would be a more targeted way to address the issue of fairness in the AI context.

***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**
We broadly agree with paragraph 79 of the CP, which suggests that defining outcome fairness in the context of data governance would not necessarily be desirable.

***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 agree**

***Q1.5.6. When developing and deploying AI, do you experience issues with identifying an initial lawful ground?***

Our members have indicated that they do experience issues with identifying an initial lawful ground. Greater opportunity to explore the legitimate interest lawful basis would be beneficial. In particular,

we welcome greater flexibility to allow for the use of a special category of data to train and develop AI, e.g. where necessary to ensure the fairness of the model.

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

Yes, particularly in relation to training and developing potentially business critical systems that necessarily require experimentation and faster delivery timelines.

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

Yes, for example in the use and re-use of data to develop new products and services for consumers.

***Q1.5.9. When developing and deploying AI, do you experience issues in other areas that are not covered by the questions immediately above?***

Yes. For example, uncertainty around risk of the ability to reverse pseudonymised data, the lawful basis for anonymising data and different levels of risk between personal data being used for AI testing and deploying AI.

***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 agree**
See our answer to Q 1.4.2.

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

**Strongly Agree**

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

**Strongly Agree**

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

We believe the following additional safeguards would be beneficial: enhanced transparency, ensuring appropriate security safeguards are in place in relation to high-risk systems, and an obligation to

conduct risk-based auditing. These measures can form part of the Accountability approach and Privacy Management Programme.

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

**Strongly agree**
We agree that the operation of Article 22 of the UK GDPR is suboptimal for the reasons outlined in the CP, and we agree that it is worth considering how to improve it, in particular in terms of more objectivity in controllers' assessments of legal or similarly significant effects on individuals.

***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'?***

**Somewhat disagree**

***Q1.5.17. To what extent do you agree with the Taskforce on Innovation, Growth and Regulatory Reform's recommendation that Article 22 of the 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?***

**Somewhat disagree**
We do not agree that Article 22 of the UK GDPR should be removed completely. We consider that it should be improved through additional contextual guidance and consultation on the key concepts. (e.g. where 'legal effects and similarly significant effects' applies).

***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.***

The CP points out that Article 22 of the UK GDPR can both under and over-regulate profiling (by excluding profiling with token human involvement or – see examples in para 97b of the CP), which is a problem. Data protection regulation seems to be the appropriate place to address profiling, but should be part of the wider, holistic legal framework including e.g. online harms and AI regulation.

We also suggest reviewing section 14 of the DPA. At present, there is no mechanism in the DPA – such as a regulation-making power – by which the UK can 'authorise' further automated decision-making use cases, as anticipated by Article 22(2)(b) of the UK GDPR. Furthermore, the safeguard in section 14 is one-size-fits-all and unlikely to be suitable for all potential automated decision-making use cases in the future; there is a risk of notification fatigue as automated decision making becomes more common.

***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 believe the current legislative transparency requirements are fit for purpose but would benefit from further nuance by way of guidance for different AI systems and use cases.

***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.***

Principles based data protection regulation seems to be a reasonable place to address data-driven harms arising from the use of AI, but should be a holistic part of the wider legal framework including e.g. online harms and AI regulation.

**1.6 Data minimisation and anonymisation**

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

**Somewhat disagree**

We consider the most appropriate mechanism to provide clarity in this area would be through the provision of regulatory guidance rather than amending the test within legislation.

This is because anonymisation is inextricably linked to the technological state of the art which may either enhance the ability to anonymise data (e.g. advanced privacy enhancing technologies) or even potentially undermine anonymisation (contrary to section 171 DPA). We therefore consider that such guidance would require updating on a reasonably frequent basis.

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

**Somewhat agree**

We consider that the re-identification test should be clarified. In particular, whether a theoretical risk that the data could be re-identified satisfies the test (thus making anonymisation only a theoretical possibility), or whether the risk has to be a practical one, taking into account the practical limits of the organisation's systems.

**1.8 Further Questions**

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

Our answer to question 1.4.2 suggests the inclusion of the categories in parts 1, 2 and 3 of schedule 1 to the DPA in the list of activities where the legitimate interests balancing test (legitimate interest assessment, or "**LIA**") would not be required. We consider that not requiring an LIA for those activities would enable organisations to more effectively facilitate DE&I activities.

Extending the definition of research to include research conducted by businesses to monitor and improve DE&I outcomes (see our answer to 1.2.3) would have an impact.

The proposal in paragraph 91b would have an impact on individuals with protected characteristics, which we believe would be positive (the proposal to create a new condition within Schedule 1 to the DPA which specifically addresses the processing of sensitive personal data as necessary for bias monitoring, detection and correction in relation to AI systems).

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

We propose that firms should be incentivised to process data for the purpose of achieving ESG and similar objectives aimed at societal benefit (for example those that come out of the COP26 conference).

The government should consider whether it would be possible to amend Parts 1 and 2 of Schedule 1 to the DPA to further DE&I objectives.

**CHP 2 - REDUCING BURDENS ON BUSINESSES AND DELIVERING BETTER OUTCOMES FOR PEOPLE**

**2.2 Reform the accountability framework**

***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 agree**

We agree that in principle, a flexible, risk-based, outcomes-focused approach to regulation is desirable. Such an approach would enable companies to align effort to underlying substantive privacy risks and focus on the protection of personal data rather than on "paper shields" that often do not substantively improve privacy compliance. This may be particularly helpful for smaller organisations.

However, there is a risk that some of the proposals (for example the removal of DPO, see below) may lessen substantive privacy compliance. Careful consideration must be given to this.

***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**

Replacing a prescriptive regime with a risk-based privacy management programme may, for some organisations, create uncertainty, require the concurrent use of multiple privacy standards across their global footprints and may undermine, rather than support, the objective of reducing barriers on organisations. The ability to adopt a consistent approach across multiple jurisdictions to implementing a privacy management programme is attractive to organisations and enables more robust implementation, rather than a fragmented approach which requires different risk-based approaches for different regions.

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

**Somewhat agree**

Currently there is no uniform approach to implementation of a privacy compliance programme. Organisations have implemented such programmes according to their specific circumstances and risks (subject to regulatory guidance). Benefits to individuals are often one, but certainly not the only, factor taken into consideration in the design and implementation of privacy management programmes.

The evolution towards a risk-based privacy management programme should not, *prima facie*, lead to a dilution of benefits to individuals. However, in order to ensure this does not happen, we would recommend that the ICO provides guidance as to what the minimum functional specification / basic requirements would be for a valid risk-based privacy management programme.

***Data protection officer requirements***

***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**
We consider there would be benefit from maintaining the requirement to designate a data protection officer ("**DPO**").

The DPO acts as the focal point for data protection compliance within an organisation including in relation to data subject communications, privacy frameworks and liaison with the ICO and in our experience, the role enhances data protection compliance. In the absence of a DPO role, the responsibilities currently being discharged by a DPO would be dispersed across the organisation and it is questionable whether large organisations would be able to manage compliance with applicable data privacy laws in as effective a manner.

In particular, the independence of the DPO role allows the office-holder to challenge the organisation's practices and is particularly helpful in ensuring compliance with data protection laws.

We note that the appointment of a DPO is only mandatory once certain criteria are met and as such, we consider the requirement to appoint a DPO to be sufficiently risk-based and proportionate.

In addition, the government should keep in mind the evolution of data protection standards globally. The role of the DPO may evolve in the future to combine with data governance or other roles to allow for greater effectiveness. Therefore, maintaining the requirement to designate a DPO maintains a sense of responsibility as the role of the DPO evolves and matures.

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

Removing the requirement under UK law to appoint a DPO may introduce operational complexities and/or may entail organisations voluntarily choosing to continue using a DPO.

Furthermore, in some cases, a DPO may be required as a matter of European law, for example when the Legacy GDPR applies or where a UK organisation triggers the territorial scope of the EU GDPR.

***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'?***

**Somewhat agree**
If properly implemented, data protection impact assessments ("**DPIA**s") can help identify, document and mitigate data protection risks as well as help drive the remediation process. A proper DPIA

methodology enables organisations to take consistent, legally accurate, defensible and auditable approach to data protection compliance relating to high-risk processing.

While the current DPIA regime has its limitations, we consider that the benefits identified above outweigh the drawbacks. The government may consider addressing the areas below to ensure that DPIAs are more effective:

- The DPIA screening criteria as set out by the GDPR, the EDPB and the ICO (pursuant to Article 35(4)) of the UK GDPR are complex, overlapping and at times confusing and are not necessarily the best tests for identifying high risk processing.
- A "one size fits all" approach to DPIAs is unhelpful insofar as it does not permit organisations to align effort to underlying privacy risk.

***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?***

**Somewhat disagree**
Instead of removing the requirement to conduct DPIAs altogether, the DCMS may consider giving the controller more flexibility (for example allowing for a risk-based approach) to decide whether a DPIA should be conducted and for determining the level of effort required for a given DPIA (e.g. having 'full' and 'standard' variations).

***Prior consultation requirements***

***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'?***

**Somewhat agree**
We agree that this proposal would in most cases act as a good incentive for effective compliance. However, it should be noted that most organisations having concluded in a DPIA that the envisaged processing would still constitute a high risk would more likely not commence the processing than approach the ICO to obtain its approval pursuant to Article 36 of the UK GDPR.

***Record keeping***

***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?***

**Disagree**
Understanding what personal data has been processed is an essential "building block" for any privacy compliance framework, useful to both the controller / processor and to the ICO. Removing the requirement may also contribute to the perception that the UK is diluting individual data subject rights.

Article 30(5) of the UK GDPR already contains exemptions from the record keeping requirements which we consider to be appropriate and proportionate.

However, we consider controllers ought to have flexibility in terms of whether to keep records of processing activities as a standalone document or whether they can be embedded into a wider information governance solution (e.g. those required by financial services regulatory obligations or by standards such as BCBS 239). This would have the advantage of enabling institutions to better operationalise their understanding of personal data processing within the context of wider data management.

***Breach reporting requirements***

***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**

We agree that the threshold for notifying personal data breaches to the ICO should be higher. We would recommend aligning the threshold for Article 33 of the UK GDPR to that within Article 34 of the UK GDPR, such that a breach is only reportable if there is a "high risk" to the rights and freedoms of natural persons. We consider that this proposal would form an integral part of the privacy management programme approach to data protection.

We consider that this would reduce the burden and costs on both the ICO and controllers, while allowing the most serious data breaches to be addressed. We recommend the ICO produce guidance, with worked examples, to clarify what constitutes "high risk".

Given the nature and extent of data sharing within the financial services industry, low level breaches do occur which present little risk to the rights and freedoms of data subjects. However given the current notification requirements, this can lead to "over-reporting" as the CP points out at paragraph 179. If the threshold were higher, we would expect for this to significantly reduce the burden on organisations whilst still ensuring that serious breaches are reported.

We would recommend retaining the obligation within Article 33(5) of the UK GDPR for a controller to document of all personal data breaches, irrespective of whether they meet the higher threshold within a revised Article 33 of the UK GDPR. This is because such a record is fundamental to an organisation's ability to identify the root causes of data breaches and to effectively remedy weaknesses in their systems. Understanding data breaches within an organisation also supports the Accountability and Privacy Programme Management objectives.

***Voluntary undertakings process***

***Q.2.2.13. To what extent do you agree with the proposal to introduce a voluntary undertakings process? As a reminder, in the event of an infringement, the proposed voluntary undertakings process would allow accountable organisations to provide the ICO with a remedial action plan and, provided that the plan meets certain criteria, the ICO could authorise the plan without taking any further action.***

**Strongly agree**
We consider the introduction of a voluntary undertaking process would lead to better protection of personal data and better outcomes for data subjects. We encourage the government to give further detail about how it envisages the proposed voluntary undertaking process would operate.

***Further questions***

***Q.2.2.14. Please share your views on whether any other areas of the existing regime should be amended or repealed in order to support organisations implementing privacy management requirements.***

See questions 2.3.1 to 2.3.5 below. We consider that the DSAR regime is in urgent need of review.

***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 disagree**
We consider the intent and use of Article 30 of the UK GDPR (namely to help organisations understand key elements of data processing) is materially different to those within Articles 13 and 14 of the UK GDPR (which are, or should, be easily-understood information for data subjects on what, why and how their personal data is processed).

***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**
It is not clear why changing the notification threshold within Article 33 of the UK GDPR would require the implementation of a new privacy management programme.

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

See questions 2.3.1 to 2.3.5 below. We consider that the DSAR regime is in urgent need of review.

**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.***

We have concerns on two distinct aspects of the data subject access request ("**DSAR**") regime:

1. Resource-intensive nature

Large companies, with complex IT application / systems architecture, often need to carry out searches which rely on expensive and resource-intensive e-discovery solutions. The costs are often wholly disproportionate to the benefit to the data subjects, which have no incentive to narrow down requests to what is strictly needed.

2. Abuse in the context of disputes

Whilst we support the policy objectives of the UK data protection legislative regime, one aspect of it – namely DSARs – has become a commonly-used (and frequently abused) weapon by litigants in disputes often totally unrelated to the protection of personal data.

ICO guidance on (for example, whether a DSAR is manifestly unfounded or excessive, or on the application of exemptions under Schedule 2 to the DPA) still permits the use of DSARs in this manner, despite it often being contrary to a Court disclosure order, often used as a "fishing expedition", or to "top up" information that individuals would not have otherwise been able to obtain from disclosure orders.

We would recommend this is addressed by either: (i) extending the interpretation of what constitutes "manifestly unfounded" to include this abuse; or (ii) the insertion of a new exemption within Part 4 of Schedule 2 to the DPA, in both cases limiting the (ab)use of Article 15(2) of the GDPR to circumstances where the data subject is genuinely concerned about the processing of their personal data and not as an alternative method for disclosure. The subjectivity of assessing whether a request is "genuinely" linked to the protection of personal data may raise some initial practical difficulty. However, we consider that this can be addressed by the courts developing precedents by dealing with individual cases on the application of either (i) or (ii).

In addition, current guidance allows data controllers to take into account the conduct of only the individual data subject in determining whether the request is "manifestly unfounded". We suggest that data controllers be allowed to factor in the conduct of third parties associated with the data subjects, such as claims management companies and law firms in coming to such a determination.

***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**

As discussed in 2.3.1 above, we would consider it appropriate to limit the application of DSARs to requests genuinely linked to the protection of personal data and to consider any other reason to be manifestly unfounded.

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

**Strongly disagree**
We are concerned that the introduction of a fee may become a barrier to data subjects exercising legitimate data subject access requests. We believe that increasing the threshold for responding to DSARs such that organisations are empowered to refuse access requests that are unrelated to data protection would be more beneficial.

***Q2.3.4. To what extent do you agree with the following statement: 'There is a case for re-introducing a small nominal fee for processing subject access requests (akin to the approach in the Data Protection Act 1998)'?***

**Strongly disagree**
We disagree. There is an existing provision to charge a fee in a limited number of circumstances (where a request is manifestly unfounded or excessive, or if an individual requests further copies of their data), which could be expanded instead of an administratively cumbersome payment process.

**2.4 Privacy and electronic communications**

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

Restrictions on analytics cookies should not include processing necessary for controllers to successfully run and develop their service offerings, which are diverse and bespoke to individual providers. This should be more narrowly defined to include non-operationally critical analytics.

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

**Somewhat agree**
We believe that simplifying cookie management practices would be beneficial to customers, as the overuse of cookie pop-ups is a barrier to a smooth web browsing experience and individuals engaging more meaningfully with cookie consent. The government should continue to carefully assess developments in the EU e-Privacy legislation in this area and adopt elements of best practice where practicable. The proposal would also enable organisations to maximise the analytics activities which could ultimately benefit customers.

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

**Somewhat agree**
We agree that consent requirements should be replaced by more principles based, broader lawful basis options. The government should continue to carefully assess developments in other jurisdictions dealing with these issues, e.g. the EU and its e-Privacy legislation and consider whether elements of best practice might be adopted in a UK context.

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

**Somewhat agree**

We believe that the overuse of cookie pop-ups is a barrier to a smooth web browsing experience and ways to allow individuals to engage more meaningfully with the use of identifiers such as cookies is required on a balanced, risk appropriate basis.

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

Yes. The government should continue to carefully assess developments in the EU e-Privacy legislation in this area and adopt elements of best practice where practicable. The proposal could mean that tailored information could be given to website users, which could provide enhanced transparency; such information could also reduce complaints.

***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?***

While this proposal streamlines and reduces the compliance burden for customers in having to set individual requirements for each service used, there is not enough alignment on standards and trackers to continue to allow a smooth user experience across websites, or deliver consolidated device/browser setting options in a risk appropriate manner. Further industry collaborating is required before this can become a widely accepted, standardised approach.

**2.6 Further Questions**

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

We would propose Article 6 of the UK GDPR be amended such that where a controller is able to rely upon a lawful basis of processing under either Article 9 of the UK GDPR (special categories of personal data) or Article 10 of the UK GDPR (criminal offence data), there should be no additional requirement to have a lawful basis of processing under Article 6 of the UK GDPR. This will remove unnecessary complexity. For example, under the current regime, a controller relying upon "substantial public interest" under Article 9(2)(g) of the UK GDPR (together with a provision under Schedule 1 to the DPA) would still be required to have a lawful basis under Article 6 of the UK GDPR. It is often unclear whether the controller may rely on Article 6(1)(e) of the UK GDPR (public interest), often leading to the requirement to undertake legitimate interests assessment despite having a strong basis in law for processing the personal data.

## CHP 3 - BOOSTING TRADE AND REDUCING BARRIERS TO DATA FLOWS

### 3.2 Adequacy

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

**Somewhat agree**

We support the adoption of a outcomes-based approach to adequacy decisions.

Further clarity on what a "risk-based" approach entails would be desirable. If the DCMS is considering mirroring the approach to Transfer Impact Assessments, by treating transfers in different sectors differently and being open to granting adequacy decisions in relation to transfers to another jurisdiction in a *particular sector* (e.g. HR data, or data used for the purpose of preventing financial crime), we would welcome such a 'risk based' approach. This more granular approach to granting adequacy decisions would reduce the need for organisations to have external legal reviews of data transfers, and reduce compliance costs.

The government should make sure that however it approaches adequacy, it should ensure that it builds and maintains the trust of individuals in data transfers.

Members expressed concerns relating to onward transfers and the UK's adequacy assessment of third countries and the impact that may have on the UK's adequacy decision from the EU. If the list of adequate countries and the onward transfer restrictions were to diverge significantly from that of the EU, then the UK's adequacy decision could be put at risk. It is also worth noting that any comprehensive adequacy finding in favour of the USA which goes beyond specific sectors or regions (e.g. California), could also be problematic in this respect.

***Q3.2.2. To what extent do you agree that the government should consider making adequacy regulations for groups of countries, regions and multilateral frameworks?***

**Somewhat agree**

Whilst we agree in principle, we consider that, in practice, the success of this approach would depend upon whether there is sufficient commonality of data protection and broader legal regimes across groups of countries and regions. Outside of the EU, we are not aware of any countries that share a completely common framework. Therefore, when considering making adequacy decisions in relation to groups of countries, the government should undertake robust due diligence following the same rigorous standards as those used in making a bilateral adequacy decision.

A particular concern is that we might endanger the EU adequacy decision if we are seen as granting less-than-robust adequacy decisions to groups of countries. Therefore, the benefit of achieving scale in adequacy decisions should be balanced against the risk that the proposal might endanger the EU and potentially other adequacy decisions.

We also encourage the government to explore multilateral solutions, for example by promoting a set of global data protection standards and / or multilateral solutions, as set out in the IRSG Report on

How the trend towards data localisation is impacting the financial services sector which can be found here: https://www.irsg.co.uk/resources-and-commentary/irsg-report-how-the-trend-towards-data-localisation-is-impacting-the-financial-services-sector/.

***Q3.2.3. To what extent do you agree with the proposal to strengthen ongoing monitoring of adequacy regulations and relax the requirement to review adequacy regulations every four years?***

**Strongly agree**

We support the proposal. The current review timeframe is not based on any objective criteria. We would recommend the criteria for ongoing monitoring are sufficiently robust such that: (i) they would be able to identify in a timely manner any changes in law or practice in a recipient jurisdiction to address substantive concerns; (iii) it would not introduce uncertainty and caution leading to an unwillingness of organisations to rely on the adequacy decision; and (iii) it would not undermine the EU adequacy decision.

***Q3.2.4. To what extent do you agree that redress requirements for international data transfers may be satisfied by either administrative or judicial redress mechanisms, provided such mechanisms are effective?***

**Somewhat agree**

We agree in principle. However, we recommend the DCMS provide more clarity on what "effective" mechanisms for redress entail. In our opinion, a waterfall mechanism whereby individuals would have to precede judicial redress by administrative mechanisms (currently not embedded in law) can be considered effective, as the administrative mechanism provides for efficient redress while the judicial mechanism provides an avenue for escalation.

**3.3 Alternative Transfer Mechanisms**

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

**Strongly agree**

We agree. As noted in the consultation, carrying out case-by-case assessments to ensure alternative transfer mechanisms are suitable in addressing the risks of the transfer (e.g., to data subject rights) is labour and time intensive, due to a large variation between different countries' regimes. A practical and detailed guide in ensuring a proportionate system is adopted when carrying out these assessments would be useful to all organisations, including both SMEs and large multinationals.

***Q3.3.2. What support or guidance would help organisations assess and mitigate the risks in relation to international transfers of personal data under alternative transfer mechanisms, and how might that support be most appropriately provided?***

**1. Provision of essential equivalence assessment**

Where an exporting organisation wishes to rely upon one of the appropriate safeguards listed in Article 46(2) of the UK GDPR (such as standard contractual clauses or binding corporate rules), it is

required by Article 46(1) of the UK GDPR to assess whether enforceable data subject rights and effective legal remedies for data subjects are available.

This includes (but is not limited to) an assessment of whether the law and practice of the importing third county is essentially equivalent to UK law. Such an assessment need only be conducted once per importing jurisdiction (or sector therein).

Such assessment is akin to conducting a quasi-adequacy decision pursuant to Article 45(2) of the UK GDPR. For reasons of legal certainty, consistency and cost efficiency, we propose that the government conduct and make available such an assessment to exporting organisations.

This would leave the exporting organisation to focus on the other more feasible aspects of the test to them as organisations – namely whether there are any factors specific to the transfer that may mitigate or exacerbate privacy risks and whether any safeguards (technical, organisational or contractual) may further mitigate such risks – being the factors that an exporting organisation is best placed to review.

***Q3.3.3. To what extent do you agree that the proposal to exempt 'reverse transfers' from the scope of the UK international transfer regime would reduce unnecessary burdens on organisations, without undermining data protection standards?***

**Strongly agree**

We agree. The current rules create compliance risks for organisations while not enhancing the protection of individuals. For example, insurance companies which operate globally usually need to engage local distributors, which have, via their trade bodies, voiced concerns that once data enters the UK, they become encumbered by UK GDPR restrictions.

We consider that exempting reverse transfers from the scope of the UK international transfer regime will undo an excessively bureaucratic burden and make the UK a more attractive destination for inbound data processing.

***Q3.3.4. To what extent do you agree that empowering organisations to create or identify their own alternative transfer mechanisms that provide appropriate safeguards will address unnecessary limitations of the current set of alternative transfer mechanisms?***

**Neither agree not disagree**

Given that data flows are an everyday occurrence for most organisations, organisations should be provided greater avenues to work with regulators to establish a suite of appropriate alternative transfer mechanisms, but these should still have regulatory oversight, rather than giving individual organisations the freedom to create any mechanism of their choosing.

Empowering organisations to work with other organisations to identify their own alternative transfer mechanisms could also lead to more innovation, for example in the use of privacy-enhancing technology to address transfer requirements.

It should however also be noted that such a function may most likely be used by large companies able to effectively design such a transfer mechanism. Those companies may be disincentivised in using such mechanisms as they seek to comply with other international regimes.

We emphasise that it would be critical for any such mechanisms to have proper regulatory oversight.

The APEC Cross Border Privacy Rules (CBPR) system is an example of organisations and governments coming together to find alternative solutions which should be encouraged.

***Q3.3.5 What guidance or other support should be made available in order to secure sufficient confidence in organisations' decisions about whether an alternative transfer mechanism, or other legal protections not explicitly provided for in UK legislation, provide appropriate safeguards?***

We consider that organisations should be given opportunities to road-test their proposed alternative transfer mechanisms and other innovations. This could be done via a regulatory sandbox or "traffic light" approach, where the ICO gives a preliminary indication to the organisations on whether their innovations are on the right track or pose regulatory compliance risks. We consider such a sandboxing approach will give organisations the confidence to continue innovating.

***Q3.3.6. Should organisations be permitted to make international transfers that rely on protections provided for in another country's legislation, subject to an assessment that such protections offer appropriate safeguards?***

**Don't know**
We would welcome further clarity on this question.

To the extent that this proposal relates to organisations' ability to use EU SCCs with the UK Addendum, we fully support such use.

To the extent that this proposal involves a test that is similar to that envisaged in Schrems II, we note that exporters, as a result of that judgment, are already required to assess (as part of the transfer impact assessment) whether the laws and practices of third countries are essentially equivalent.

If the proposal envisages something different, further clarity would be desirable.

***Q3.3.7. To what extent do you agree that the proposal to create a new power for the Secretary of State to formally recognise new alternative transfer mechanisms would increase the flexibility of the UK's regime?***

**Somewhat agree**
We agree, but there should be consultations before a new alternative transfer mechanism is recognised. Recognition of new alternative transfer mechanisms via Secondary Legislation may also offer sufficient flexibility while also retaining Parliamentary oversight.

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

**Yes**
See our response in 3.3.5. We also recommend an incubation period in which organisations can work with the government to explore what innovations in the alternative transfer mechanisms sphere are feasible.

**3.4 Certification Schemes**

***Q3.4.1. To what extent do you agree with the approach the government is considering to allow certifications to be provided by different approaches to accountability, including privacy management programmes?***

**Strongly agree**
The privacy management programmes would be a good basis for certifications.

***Q3.4.2. To what extent do you agree that allowing accreditation for non-UK bodies will provide advantages to UK-based organisations?***

**Strongly agree**
This has the potential to strengthen the international rules based system, and put the UK in the lead for developing a future international data transfer framework. In addition, the government should be mindful that it may be open to accusations of trade discrimination if non-UK bodies are not allowed accreditations.

***Q3.4.3. Do you see allowing accreditation for non-UK bodies as being potentially beneficial for you or your organisation?***

**Strongly agree**

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

Encouraging the UK's international partners to follow suit, and encouraging the authors of certification regimes to engage with as many other governments as possible.

Cooperation with other UK regulators in this space, perhaps through the Digital Regulation Cooperation Forum. This would allow certifications to cease to concern only privacy issues but instead enable a broader view of data and work across sectors.

**3.5 Derogations**

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

**Strongly agree**
We do not consider the transfer mechanisms within Article 49 of the UK GDPR to be a material dilution of privacy protection compared to other transfer mechanisms. The current approach under

the EU and UK GDPR is rigid and often creates uncertainty as to what constitutes 'repetitive transfers.'

We would therefore invite the government to consider: (i) removing the mandatory cascading, or "waterfall", whereby the transfer mechanisms within Article 49 of the UK GDPR may be used only "[i]n the absence of an adequacy decision … or appropriate safeguards"; and (ii) consider reframing the provisions within Article 49 of the UK GDPR such that they are considered as legitimate, rather than last resort, transfer mechanisms.

**3.6 Further Questions**

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

As noted in our response to question 3.3.5, we encourage the government to create a regulatory sandbox mechanism where organisations are able to road-test their ideas on alternative transfer mechanisms with the ICO. To reduce the burden on the ICO, it may be appropriate to introduce a reasonable fee payable by organisations who would like to participate in the sandboxing.

To achieve digital transformation, the government should be open to, and furthermore encourage new opportunities for organisations to use data responsibly - for example, to achieve ESG or D&I objectives. The government may consider maintaining an open dialogue and continued support for the use of data in innovation.

**CHP 4 - DELIVERING BETTER PUBLIC SERVICES**

**4.2 Digital Economy Act 2017**

***Q4.2.1. To what extent do you agree with the following statement: 'Public service delivery powers under section 35 of the Digital Economy Act 2017 should be extended to help improve outcomes for businesses as well as for individuals and households'?***

**Somewhat agree**
We agree in principle and ask the government to bring forward more specific proposals.

**4.3 Use of Personal Data in the COVID-19 Pandemic**

***Q4.3.1. To what extent do you agree with the following statement: 'Private companies, organisations and individuals who have been asked to process personal data on behalf of a public body should be permitted to rely on that body's lawful ground for processing the data under Article 6(1)(e) of the UK GDPR'?***

**Strongly agree**
We agree, as organisations are reluctant to process personal data on behalf of a public body due to uncertainty over the appropriate lawful basis. This proposal should be subject to upstream checks to ensure lawful basis of processing will continue to be valid grounds for processing by other third parties. Being able to rely on a public body's own lawful basis would likely mean that organisations would have less uncertainty about whether they were able to comply with such requests.

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

As above

***Q4.3.3. To what extent do you agree with the proposal to clarify that public and private bodies may lawfully process health data when necessary for reasons of substantial public interest in relation to public health or other emergencies?***

**Strongly agree**

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

We believe strong safeguards exist.

**4.4 Building trust and transparency**

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

The public and private sector duties should be aligned.

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

**Strongly agree**
See question 1.4.2. In particular we would support the expansion of paragraph 9 of Schedule 1 to cover diversity in relation to all current and any potential future protected characteristics, and not just racial and ethnic diversity at the senior level of an organisation. This gives organisations more flexibility to process sensitive data to achieve DE&I purposes.

A condition permitting use of special category data for detection, investigation and prevention of economic crime in all its evolving forms would be welcome. This would be broader than the existing SPI condition for 'preventing fraud' and would be helpful.

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

**Strongly agree**
In our response to question 2.6.2, we noted the overlap between Articles 6 and 9 of the UK GDPR, and that under current rules, organisations that rely on "substantial public interest" under Article 9(2)(g) of the UK GDPR are not clear as to whether they can also rely on "public interest" under Article 6(1)(e) of the UK GDPR.

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

**Strongly agree**
We agree. We welcome a definition of the term as well as guidance setting out examples of circumstances in which "substantial public interest" can be relied upon. Regarding the formulation of the definition, we consider that achieving ESG and DE&I objectives should be considered as "substantial public interest".

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

**Strongly agree**
See question 1.4.2. In particular we want to expand paragraph 9 of Schedule 1 to the DPA to cover diversity in relation to all current and any potential future protected characteristics, and not just racial and ethnic diversity at the senior level of an organisation. This gives organisations more flexibility to process sensitive data to achieve DE&I purposes.

In addition, the government should remove the circularity in Schedule 1 to the DPA whereby it is a requirement to demonstrate that processing "is necessary for reasons of substantial public interest"

where, pursuant to Article 9(2)(g) of the UK GDPR and section 10(3) of the DPA, the provisions within Schedule 1 Part 2 of the DPA are meant to list the conditions for substantial public interest to be satisfied.

**CHP 5 - REFORM OF THE INFORMATION COMMISSIONER'S OFFICE**

**5.2 Strategy, Objectives and Duties**

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

**Neither agree nor disagree**

Regardless of how the statutory framework is structured, the functional and regulatory independence of the ICO provides value in creating confidence in the fairness of the discharge of its functions, thereby facilitating the UK's position as a leading jurisdiction for data and reinforcing public and business confidence. There is a fine balance to be struck between appropriate and democratic political direction and procedural fairness and independence. We consider that maintaining the benefits of the ICO's independence should be a key priority for the government as a matter of good regulatory practice.

***Q5.2.5. To what extent do you agree with the proposal to introduce a duty for the ICO to have regard to competition when discharging its functions?***

**Somewhat disagree**

Whilst we can see some merit in this approach, there is a risk of dilution of the key objectives of the data protection regime. Other regulators, which have singular or concurrent jurisdiction over *ex ante* and / or *ex post* competition policy regulation of various industries, may be better placed to have regard to competition.

***Q5.2.6. To what extent do you agree with the proposal to introduce a new duty for the ICO to cooperate and consult with other regulators, particularly those in the DRCF (CMA, Ofcom and FCA)?***

**Somewhat agree**

There should be mutuality in the cooperation and consultation obligations such that other regulators, particularly those in the DRCF, also have a duty to consult and cooperate with the ICO.

***Q5.2.8. To what extent do you agree with the establishment of a new information sharing gateway between relevant digital regulators, particularly those in the DRCF?***

**Strongly agree**

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

Please see answer to question 5.2.1.

**5.4 Accountability and Transparency**

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

**Somewhat agree**
We agree that what the ICO discloses needs to be transparent and open. We also recognise that in order to grow the trust and facilitate candid dialogues between organisations and the ICO, the ICO should be mindful and proportionate in exercising its powers.

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

In relation to enforcement action, the ICO should publish its policies, and clear rules and guidance setting out the processes of how such actions are taken.

**5.5 Codes of Practice and Guidance**

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

**Strongly agree**

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

**Strongly agree**
We agree, and the DCMS should ensure that businesses are adequately represented on the expert panel.

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

**Strongly disagree**
We are concerned that giving the Secretary of State a role in approving codes of practice and complex and novel guidance may be seen as impinging on regulator independence. Please also see answer to question 5.2.1. In addition, the independence of the ICO is one of the major factors in the European Commission's methodology for adequacy assessment. We are concerned that any perceived encroachment of the ICO's independence may endanger the EU and potentially other adequacy decisions.

**5.6 Complaints**

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

We consider that the ICO has already taken a proportionate approach to data protection 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**

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

**Somewhat disagree**
Most data controllers already have a complaints handling process in place, and it is not clear what the proposal adds to the current practice, other than requiring the data controller to publish the complaints handling procedure.

We consider that this proposal increases organisations' regulatory burden without identifying a problem that needs to be addressed. The government should provide more information on the mischief that this proposal is intended to remedy.

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

**Neither agree nor disagree**
The government should clarify what the ICO taking a "risk-based approach" to complaints means.

**5.7 Enforcement Powers**

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

**Strongly agree**

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

**Somewhat agree**
In principle we understand why the ICO wants to commission technical reports to inform investigations. However, we suggest that the ICO focus its resources on other material issues in the investigation and set a materiality threshold for the commissioning of the technical reports.

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

We do not consider it appropriate for the organisations to bear the costs of the technical reports, as this would create a moral hazard: the ICO would not be incentivised to limit the commissioning of

technical reports to material cases, as it does not bear the full costs of doing so. We consider that the ICO should bear the cost, and that combined with the materiality threshold suggested in question 5.7.2, this will encourage the ICO to commission technical reports only when necessary and proportionate. Organisation will also not be subject to an unfair financial burden.

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

See question 5.7.3

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

**Somewhat agree**
We agree in principle, however the power to compel witnesses to give evidence is an exceptional one, with implications on fundamental freedoms and individual rights.

We note that other regulators in the DRCF do have the power to compel witnesses to attend interviews. Ofcom, for example, is empowered by section 26A of the Competition Act to require an individual connected with the subject of the investigation to answer oral questions on any matter relevant to the investigation. The CMA has the power, under section 109 of the Enterprise Act 2002, to require persons to give evidence and to provide specified documents and information needed for the purpose of a merger inquiry. Non-compliance may result in a monetary penalty subject to a right to appeal to the CAT. As noted in the Consultation Paper, FCA also has the power to require the person under investigation, or any connected person to attend an interview or to provide information.

We encourage the government to review the relevant powers in relation to other regulators and implement safeguards to ensure that this proposed power is not misused if created.

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

See above.