DCMS Consultation ‘Data: a new direction’ 10 September 2021 Response by Robert Baugh

This is a response to the Department for Digital, Culture, Media & Sport’s Public consultation on reforms to the UK’s data protection regime, published on 10 September 2021, and which closes at 11:45pm today, 19 November 2021 (‘**Consultation**’ and the proposals set out within the Consultation ‘**Proposals**’).

Contents

About this Response

Respondent's details

Name: Robert Baugh
Email address: robertb@keepabl.com

Respondent's Relevant Experience & Expertise

A UK citizen living in London, I qualified as a Solicitor in England & Wales in 1995, I later qualified in Hong Kong (now non-practising), and have twice been shortlisted for In-House Lawyer of the Year in the Law Society Excellence Awards. After nearly a decade as a technology lawyer in City firms in London, Hong Kong and Melbourne, I spent over a decade as General Counsel of VC-backed international growth technology companies before founding Keepabl Ltd. I have therefore been advising on, speaking on, writing on, and involved in data protection law for over 25 years.

Keepabl is award-winning Privacy Management Software with customers in industries from Finance to Publishing, Tech to Charities and with customers in the UK, EEA and elsewhere. Our SaaS solution and Privacy Policy Pack provide a complete Privacy Framework focussed on GDPR. Keepabl's aim is to make compliance (in particular operationalising Privacy and Security) as intuitive and simple as possible for our customers. We welcome any measures and initiatives that make compliance easier for organisations. We also publish the Privacy Kitchen free video channel with help on GDPR and all things Privacy.

I am therefore an expert in data protection law, international commercial law and practice, and a UK-based technology founder.

Personal view only

This response is the personal view of Robert Baugh only and is not submitted on behalf of, nor does it necessarily represent the views of, Keepabl Ltd.

Structure of this Response

This response follows the structure of the Consultation and I have responded to questions in that order. While I have responded to the majority of questions, I have not responded to questions where I feel my experience or expertise is not so relevant, or where my other responses have made the question 'not applicable'.

Summary

I believe I have a very apposite experience and expertise from my own legal and practical knowledge of Privacy compliance and my qualitative experience in the marketplace: advising organisations on Privacy compliance; creating, marketing and selling a leading Privacy Management Software solution to organisations (public and private); and listening to and discussing Privacy with experts in the operational aspects of Privacy compliance.

In the context of my knowledge and experience, I see the bulk of the Consultation, Proposals, and related documents such as the TIGGR report, as:

- heavily (and presumably politically) biased against the EU GDPR,
- based on an inaccurate view of the operational realities of implementing Privacy compliance for the EU and UK GDPRs and other relevant laws, and
- contrary to most surveys and even contrary to recent government firmly-held positions.

I do not believe the Proposals can be confidently said to deliver any benefit to British data subjects (quite the reverse) nor British organisations, save for the Proposals:

- on the risk level for notifying the UK ICO of a personal data breach, and
- on reviewing the DPO role.

As a technology founder, I am still witnessing European prospects wary of UK-hosting, preferring EEA hosting for continuity - because the UK continues to act in a way that puts the adequacy decision in peril.

Far from being seen as a trusted hub for personal data, I believe European Privacy professionals and organisations see the UK with a great deal of wariness, as a nation that has not for some years been a source of confidence and consistency, and looks to be perpetuating the uncertainty for some years to come. For that reason, I believe the UK government's approach to data protection since 2018 has significantly damaged the UK's standing on data protection, reduced opportunities for British businesses, and correspondingly increased opportunities for EEA businesses.

As well as Brexit, Covid-19 and the related lockdown have impacted Britain's economy. The Office for Budget Responsibility's statistics suggest a 2% hit to GDP from Covid (which should recover quickly) and a 4% hit to GDPR from Brexit (which will not) after '[t]he UK economy recorded its worst economic performance for more than 300 years.' The value of trade with the EEA dependent on personal data flows is well-known, and noted by the government itself.

Deliberately introducing uncertainty to this degree, instead of removing uncertainty and providing confidence in at least one area of regulation, is not beneficial to the British economy nor the British people. In these times of poverty levels staying the same or increasing (particularly child poverty), and increasing income and wealth inequality, there are many better uses of public funds and resources for the benefit of the British public and state than this Consultation.

The Introduction & Ministerial Letter

Macro- and Micro-Economic Context

Apart from a data protection viewpoint, there are significant economic arguments against carrying out the Proposals save for those above. As above, the Office for Budget Responsibility's statistics suggest a 2% hit to GDP from Covid (which should recover quickly) and a 4% hit to GDPR from Brexit (which will not) after '[t]he UK economy recorded its worst economic performance for more than 300 years.'

Economists and business people prefer certainty over uncertainty. Brexit introduced a lengthy period of a high level of uncertainty for businesses in the UK, EEA and around the world in terms of whether the UK would remain a compliant location for the hosting of personal data. Since GDPR became applicable in 2018, I have personally witnessed European and other businesses (both providers and customers) deciding to move their personal data into Germany, Ireland or other EEA member state to remove the need to spend the following years in a state of anxiety about a key plank of their Privacy compliance.

I believe that movement of databases only consolidated since 2018, spurred on by continued debate about whether the UK would receive an adequacy decision, the untimely publication of the TIGGR report, and with even many UK commentators (excluding the respondent) stating that the UK did not deserve an adequacy decision.

I believe the Proposals put the UK Adequacy Decision in serious jeopardy. In April 2021, before the adequacy decision in favour of the UK, the EU Parliament stated (our emphasis):

> '*However, due to lack of agreement on data transfer conditions* ***and possible divergence in data standards****, the parties were unable to implement sustainable solutions, such as long-term trade rules or an adequacy decision under the General Data Protection Regulation (GDPR).* ***A recent study estimated the costs of 'inadequacy' at around GB£1-1.6 billion (€1.116-1.7856 billion) for UK firms****, stemming largely from companies reverting to alternative transfer mechanisms under the GDPR*.'

Page 9 of the Consultation says:

> *'19. ... Our initial economic analysis shows that our reform package will have a net direct monetised benefit of £1.04 billion over 10 years, even after accounting for potential costs incurred through any future changes to the UK's EU adequacy decisions.'*

The ONS states that UK GDP in Q3 2021 was £553,412m. If correct, the Consultation's figure of £1.04bn over 10 years would equate to £26m per quarter, or just 0.005% of GDPR.

In the government's pre-GDPR, post-Brexit-vote paper, The exchange and protection of personal data, a Future Partnership Paper, it states (our emphasis):

> *'6. Increasingly, data flows envelop all trade in goods and services as well as other business and personal relations. The UK is a significant player in global data flows. Estimates suggest that around 43 per cent of all large EU digital companies are started in the UK[3], **and that 75 per cent of the UK's cross-border data flows are with EU countries**.[4] Analysis indicates that the UK has the largest internet economy as a percentage of GDP of all the G20 countries[5], and has an economy dominated by service sectors **in which data and data flows are increasingly vital**. The UK accounted for 11.5 per cent of global cross-border data flows in 2015, compared with 3.9 per cent of global GDP and 0.9 per cent of global population[6], but the value of data flows to the whole economy and the whole of society are greater still.*
>
> *7. **Any disruption in cross-border data flows would therefore be economically costly to both the UK and the EU.** Taking EU-US data flows as a comparator, external estimates suggest that if cross-border data flows between the EU and the US were seriously disrupted, the EU's GDP could reduce by between 0.8 and 1.3 per cent.[7] Therefore, placing restrictions on cross-border data flows could harm both the economies of the countries implementing these policies, as well as others in the global economy.'*

TIGGR's report, quoting the DCMS Sectors Economic Estimates 2018 (provisional): Gross Value Added report, in paragraph 203, recognises that:

> *'In 2018, the digital sector contributed £149 billion to the UK economy—equivalent to £400 million a day. Growth in the sector is nearly six-times larger than growth across our economy as whole.'*

Deliberately putting at risk the free flow of personal data with the EEA, for the benefit of free transfer of personal data to the US, Kenya and other countries whose data protection regimes are either positively unacceptable to the EU, or yet to be reviewed as adequate (almost the same thing in practice since *Schrems II*), seems illogical particularly at this time of economic fragility and given what I see as the clear negative aspects of the Proposals.

GDPR is no bar to innovation or emergency sharing

The Consultation makes much of the need to share personal data, using the reaction to Covid as an example, implying that GDPR is a barrier. However, as the UK ICO stated on 12 March 2020:

> '*Data protection and electronic communication laws do not stop Government, the NHS or any other health professionals from sending public health messages to people, either by phone, text or email as these messages are not direct marketing. Nor does it stop them using the latest technology to facilitate safe and speedy consultations and diagnoses. Public bodies may require additional collection and sharing of personal data to protect against serious threats to public health*.'

And on 17 April 2020:

> *'But, as with any new technology, the public need to have confidence that it is being used in a fair and proportionate way. Our statement on coronavirus in March made the point that data protection laws do not get in the way of innovative use of data in a public health emergency – as long as the principles of the law (transparency, fairness and proportionality) are applied. The same approach applies to the use of contact tracing applications.'*

The rules on data protection in a Covid context were perfectly clear; the UK government's messaging was not. For example, there was widespread belief that collection of customers' personal data at bars and restaurants was compulsory when it was not. And the UK ICO (usually very timely with practical advice) was extremely late to offer practical advice, when there were very good examples such as the clear work and advice from the New Zealand regulator on how access to venues could be monitored without personal data being passed to the venue itself. The advances and innovation in New Zealand and elsewhere would have been very helpful in delivering clarity to UK businesses and the public.

The EU GDPR Adequacy Decision in favour of the UK

The Minister's letter states:

> *'[The reforms] also align with our plans to drive forward ambitious data adequacy agreements with other leading economies.'*

Further, page 8 of the Consultation states:

> *'15. In that spirit, the government believes it is perfectly possible and reasonable to expect the UK to maintain EU adequacy as it begins a dialogue about the future of its data protection regime and moves to implement any reforms in the future. European data adequacy does not mean verbatim equivalence of laws, and a shared commitment to high standards of data protection is more important than a word-for-word replication of EU law. Indeed, other countries, such as Israel, have been granted adequacy decisions by the EU while pursuing independent and varied approaches to data protection, reflecting their unique national circumstances, cultures and heritages.'*

Among factors to be taken into account for an adequacy decision are the UK's approach to transfers. Prioritising countries which the EU has not found adequate (or have found the opposite) will most likely increase uncertainty over the validity and longevity of the adequacy decision and incentivise further movement away from hosting personal data in the UK.

Comparing the UK with New Zealand or Israel is not a valid comparison - we are starting from a position of already matching the EU GDPR. We have understood the processes, much of which were there in the 1995 EU Data Protection Directive and UK Data Protection Act 1998, for a long time. Other countries have to change their regimes to move closer to the EU GDPR. It appears illogical, when EU GDPR is driving data protection law reform around the world, that the UK should be almost the only country looking to move in the opposite

direction. This will place additional burdens and disadvantages on UK businesses to change yet again for no proven benefit and major risk and uncertainty.

Incorrect View of GDPR & Privacy Compliance Programs

The Introduction presents GDPR as an entirely new and unknown law, ignoring the fact that much of GDPR, including its underlying principles and rules, have been in UK and EU law for decades. This biased messaging from the government, contrary to its own prior statements, and lack of awareness of how organisations are currently operationalising Privacy, do not positively impact the UK's desired position as a trusted hub for data protection.

Contrary to the government's statements in 1.1, I believe the principles and rules in GDPR are very well known.

- The majority were in the 1995 EU Data Protection Directive and the 1998 UK Data Protection Act, which is unsurprising as they're set out in the legally-binding Convention 108 from 1981, which the government refers to in the Consultation.
- Much of the Article 29 Working Party Guidelines and other papers have been approved by the EDPB and the UK ICO's various guidance has hardly changed.

The fines have changed, and made people look at the rules properly for the first time. An exacerbating issue has been that there were not enough experts on the regime pre-GDPR given the sudden increase in public and organisational demand for Data Protection advice post-GDPR.

Lawful Grounds

As a further example of what I believe is an incorrect 'polar opposite' view of GDPR in the Consultation, Page 11 of the Consultation, paragraph 30, states:

> *'The government has also heard evidence that uncertainty about when different lawful grounds for processing personal data should be used has led to an overreliance on seeking consent from individuals.'*

I note there is no statistically relevant survey for this statement which is the contrary to all I have heard from organisations and advisors - consent used to be the lawful ground that everyone relied on pre-GDPR but since GDPR tightened the recording and reporting conditions on consent, organisations are doing everything they can to avoid using it.

This view is also in TIGRR's report, paragraph 209:

> *'GDPR is centred around the principle of citizen-owned data and organisations generally needing a person's 'consent' to process their data. There are alternative ways to process data that do not require consent, but these are not well defined or understood, causing confusion amongst data processors and controllers.'*

I believe this is wholly incorrect and displays an embarrassing lack of knowledge of the subject matter. For example, how can 'necessary for a legal obligation' be misunderstood?

TIGRR also conflates the e-Privacy Directive (and PECR) with GDPR in its discussion of cookie banners. In paragraph 215, it states:

> *'A good measure of whether reform is successful will be the end of pointless cookie banners, together with securing a greater understanding among the public of how their data is used, if and how they benefit from their data and what their realistic privacy and consent powers really are.'*

Cookie consent tools have indeed become far more prevalent but the ICO has hardly enforced against the legion of major publishers who incorrectly, and in breach of PECR and GDPR, use such tools. For example, there is no legitimate interest basis for using cookies and similar technologies yet many large publishers preset such cookies. Following the French and other regulators' practices, it would be easy for the ICO to take action against such publishers and change the practice to be more compliant, much as they act under PECR. Driving more compliant cookie consent settings would also answer the risk of cookie consent fatigue and improve public confidence in the same.

Article 30 Records

In paragraph 176, on Article 30 Records, the Consultation states:

> *'This requirement can involve the creation of large amounts of paperwork, which largely duplicates information required by other provisions in the legislation, particularly the requirement to provide information to data subjects in Articles 13 and 14 of the UK GDPR. In addition, as part of a privacy management programme, an organisation would be required to have in place measures which assist the designated responsible individual for structuring an appropriate privacy management programme and demonstrate the organisation is compliant with data protection legislation. This includes having personal data inventories which explain what personal data is held, where it is held, why it has been collected and how sensitive it is (see paragraph 156a(III)).'*

The Consultation here displays a lack of knowledge of how Privacy programs work in practice, in suggesting Privacy notices under Arts 13 and 14 and the Article 30 Records are a duplicative process.

One cannot create Privacy notices if one hasn't made an inventory of processing activities and the lifecycle of the personal data - which you also stress is a key part of any Privacy management program. The Art 30s are simply the tip of the iceberg, where the iceberg is the organisation's full personal data inventory - which, analogous to the Information Asset Register and other registers for Security, is the fundamental part of any Privacy program.

SaaS solutions such as Keepabl (I admit there are others) instantly create the Article 30 Records from the personal data inventory without a single step by the customer.

Recitals

As another example, the government appears to be stating that having Recitals in the law is a new thing and introduces uncertainty in a new manner. The 1995 DP Directive had 72 Recitals and 34 Articles - more than twice the number of Recitals than Articles. The GDPR has 173 Recitals and 99 Articles.

Business comfort with GDPR

The Consultation paints GDPR as totally new, vastly unpopular, with negative impacts and almost impossible to understand.

As to how businesses are handling GDPR, the DCMS's own survey (DCMS, UK Business Data Survey 2020 Summary Report, May 2021, page 9) stated:

> *'Around two thirds of UK businesses that collect personal data said they have a privacy management framework or data protection strategy in place.'*
>
> *'Of the subgroup of those that have employees, the vast majority (93%) felt that their employees were proficient in handling personal data.'*

Marketing might be seen as an area most affected by GDPR. As early as 2019, the Data & Marketing Association's report, Data Privacy: An Data Privacy : An Industry Perspective, stated in the Introduction on page 3 (our emphasis):

> *'With an eye on 2020 and beyond, GDPR should be seen as bringing* ***welcome stability and legislative homogeneity*** *as we build a new relationship with the EU and ensure the free flow of data. Whatever that relationship eventually looks like, marketers understand and are concerned about the impact of losing access to the 'Digital Single Market' on our industry.'*

And their findings includes (our emphasis):

- *Less than one in 20 marketers believe GDPR has had a negative impact or made things worse across a range of key areas*
- *32% of respondents think the law has generally improved their business, 25% believe increased customer trust is a connected effect; 22% say it has improved customer relationships*
- ***Some 59% of marketers want future data laws to be stricter than the GDPR, compared to just 11% a year ago***

Similarly, the DMA's Marketer Email Tracker 2019 suggested that marketers were then feeling '*broadly positive*' about GDPR and estimated that '*ROI for every pound spent on email reached £42.24 in 2018, up from £32.38 in 2017.'*

This comment on stricter laws is interesting as a recent, 2021, KPMG US survey (in the US) revealed that:

- 29% of those surveyed admitted that their company sometimes employs unethical data collection methods,
- 33% said consumers should be concerned about how their personal data is used by their company, and
- 62% said their organisation should be doing more to strengthen existing data protection measures.

Returning to the DCMS's own survey (DCMS, UK Business Data Survey 2020 Summary Report, May 2021, on page 10, our emphasis):

> *'**A substantial proportion of respondents felt that there had been benefits to their business from the implementation of GDPR** and DPA 2018, with only around a quarter saying that there had been no benefits'*

Chapter 1- Reducing barriers to responsible innovation

The government welcomes views on the following questions:

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q1.3.1: Strongly disagree. This is clear, with a clear compatibility test.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly 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*

RB response Q1.3.2: Somewhat agree, however as the UK ICO stated, GDPR does not prevent use in an emergency situation and there is high risk of scope creep on this proposal which, if passed would need to be tightly circumscribed so it is not abused by private and public sector actors.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q1.3.3 and Q1.3.4: Strongly disagree. The rules on transparency and sharing are fundamental and straightforward. These proposals (in the context of the text preceding them) hugely increase the risk of invisible processing.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q1.4.1 and 1.4.2: Neither agree nor disagree. I believe that the examples given are almost all acknowledged as being valid legitimate interests if a balancing test is passed. And a balancing test, even a very informal one, is an appropriate risk control mechanism. There could be a rebuttable presumption that the grounds stated pass a balancing test, unless there are unusual facts, context or vulnerable data subjects, in which case there is no presumption.

Again, as above, I do not recognise this over-reliance on consent. I routinely hear (and advise) reliance by private sector on legal obligation, followed by contract, followed by legitimate interests, then consent as a last resort.

Q1.4.4. To what extent do you agree that the legitimate interests balancing test should be maintained for children's data, irrespective of whether the data is being processed for one of the listed activities?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q1.4.4: Strongly agree. Children - and other vulnerable data subjects - need an extra level of care and protection.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q1.5.1: Somewhat agree.

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?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q1.5.2: Somewhat disagree.

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?

RB response Q1.5.3: The various regulators all have expertise in their respective fields (equality, data protection, etc). I recommend maintaining the status quo and encouraging and enabling closer cooperation such as via MOUs entered into by the ICO with the FCA and other regulators, and monitoring where improvements may be made.

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?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q1.5.4: Somewhat agree. As above, it feels too early to do so.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q1.5.5: Strongly disagree. The low levels of compliance with the 1998 Data Protection Act and the 2018 Data Protection Act / UK GDPR would only be compounded by relaxing the laws on use of personal data for AI. The UK ICO regularly notes that GDPR does not impinge but enables innovation.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q1.5.10: See my answer to 1.4.2 to 1.4.4 above.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q1.5.11: Somewhat disagree. The rules are clear. That they are not always supportive of a desire to develop a particular technology does not make them unclear.

> *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*
> - *Somewhat agree*
> - *Neither agree nor disagree*
> - *Somewhat disagree*
> - *Strongly disagree*

RB response Q1.5.12: Somewhat disagree. See my answers to 1.4.2 to 1.4.4 and 1.5.11 above.

> *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*
> - *Somewhat agree*
> - *Neither agree nor disagree*
> - *Somewhat disagree*
> - *Strongly disagree*

RB response Q1.5.12: Insufficient information on the government's considerations to respond.

> *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'?*
>
> - *Strongly agree*
> - *Somewhat agree*
> - *Neither agree nor disagree*
> - *Somewhat disagree*
> - *Strongly disagree*

RB response Q1.5.16: Somewhat agree. I strongly disagree that human involvement '*may, in future, not be practicable or proportionate*' in cases with legal or similarly significant impacts on individuals, not least given how inaccurate such systems are. This part of the Consultation appears to run contrary to the stated aim to keep protection of individuals at the centre of data protection laws and reforms.

> *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 agree*
> - *Somewhat agree*
> - *Neither agree nor disagree*
> - *Somewhat disagree*
> - *Strongly disagree*

RB response Q1.5.17: Strongly disagree. Such systems are wildly inaccurate at present, see below, and human review should be retained for legal or similarly significant potential impacts.

The Moorfields Eye Hospital example is a rare example of supremely 'clean' data. Most data is quite 'dirty' data and the models use datasets that are not relevant or have inbuilt bias (see, for example, Atlas of AI and other publications by Kate Crawford, Research Professor at USC Annenberg, a senior principal researcher at Microsoft Research, and the inaugural chair of AI and Justice at the École Normale Supérieure and see New Yorker). Other references:

Big Brother Watch:

- 'The overwhelming majority of the police's 'matches' using automated facial recognition to date have been inaccurate. On average, a staggering 95% of 'matches' wrongly identified innocent people.
- Police forces have stored photos of all people incorrectly matched by automated facial recognition systems, leading to the storage of biometric photos of thousands of innocent people.'

BBC News
Sky news: Met Police 81% error rate.

> *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.*

RB response Q1.5.18: Profiling is one of the less understood yet major themes in GDPR at present - and in any legislation. AI, the use of training data, profiling, real-time bidding (RTB), invisible processing and more are all hot topics at present. One needs to be careful of looking at the issue from the viewpoint of 'I want business to do this, so how can we change the law' instead of 'we need to protect individuals, is the law sufficient?' The UK proposals seem to take the former approach, the EU more so the latter (but not always). Therefore, I suggest the impact of GDPR on profiling has yet to be felt, largely due to poor enforcement, and the law should stay as is for now.

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).

RB response Q1.5.19: Legislative action is not necessary, enforcement is.

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.

RB response Q1.5.20: It is one, but should not be the only one. As Lloyd -v- Google illustrates, there are various 'hooks' you can 'hang a case on' and exclusivity over such actions should not be legislated at this time.

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?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q1.6.1: Strongly disagree. There is no need to do so to give effect to this, therefore this Proposal is is not a relevant use of the legislature's time and resources.

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

- *Recital 26 of the UK GDPR*
- *Explanatory Report to the Modernised Convention 108+*
- *N/A - legislation should not be amended*
- *Other*

RB response Q1.6.2: Recital 26 is a practical solution at present.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q1.6.3: Somewhat agree.

> *Q1.6.4. Please share your views on whether the government should be promoting privacy-enhancing technology, and if so, whether there is more it could do to promote its responsible use.*

RB response Q1.6.4: This would be beneficial, however it is fraught with risk of corruption where officials can provide 'imbalanced' support to certain organisations - and there are plenty of examples at present of officials lobbying for personal reasons.

Any such help should be delivered in ways that meet an exacting standard of impartiality. Best practice from overseas can help. For example, the New Zealand Privacy Commissioner created a Privacy friendly badge for solutions of various levels of technology to obtain.

> *Q1.7.1. Do you think the government should have a role enabling the activity of responsible data intermediaries?*
> - *Yes*
> - *No*
> - *Don't know*

RB response Q1.7.1: There are possibly three main reasons why data sharing might occur:
- for the immediate benefit of data subjects (the Open Banking examples you give, making it easier for data subjects to connect the services they want);
- to allow for commercial opportunity; and
- to benefit the public as a whole (the Covid examples you give).

Data Protection law of any flavour recognises the primacy of the first and third scenarios above, with the second commercial scenario subject to the condition that nothing harms the rights and freedoms of data subjects.

I believe current law provides the legislative framework to allow for other examples along the lines of Open Banking and the Covid example you give, without the need for change.

> *Q.1.7.2. What lawful grounds other than consent might be applicable to data intermediary activities, as well as the conferring of data processing rights and responsibilities to those data intermediaries, whereby organisations share personal data without it being requested by the data subject?*

RB response Q1.7.2: I see none, save for public interest such as the Covid examples you provide. Any sharing by private entities for their own pursuit of commercial enterprise is contrary to Data Protection law principles without consent else there is the high risk of invisible processing of the type the UK ICO detailed in its enforcement notice against Experian.

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)?

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?

RB response Q1.8.1 and 1.8.2: I see no barrier under current data protection law that can be removed without significant degradation of the rights and freedoms of data subjects.

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

In para 139 on page 53, the Consultation states:

> *'Although a key goal of the EU's GDPR was to create a regime that focussed on the accountability of organisations, the current model, in practice, tends towards a 'box-ticking' compliance regime, rather than one which encourages a proactive and systemic approach, and risks undermining the intentions of the principle of accountability. A largely one size-fits-all approach from organisations, regardless of the relative risk of their data processing activities, can potentially discourage innovation in how to achieve the actual goals of using data responsibly and protecting individuals' rights.'*

This is not a fair description of the GDPR nor the 1995 Directive before it, as the UK government itself strongly stated in The exchange and protection of personal data, A Future Partnership Paper, paragraph 13 on page 4 (our emphasis):

> *'**The UK played a full and active part in negotiations for the new GDPR** and DPD, and the final text reflects a number of key UK priorities. **For instance, the GDPR takes a more risk based approach than had previously been adopted, with the result that certain obligations with which data controllers must comply are proportionate to the risk posed by the data processing activity**. The GDPR and DPD were adopted in 2016 and are due to come into force in May 2018 (replacing the 1995 Directive), before the UK leaves the EU. The new rules strengthen rights and empower individuals by giving them more control over their personal data.[9]'*

In para 145 on page 54, the government states it believes, under its proposals:

> *'organisations would be required to implement a privacy management programme tailored to their processing activities and ensure data privacy management is embraced holistically rather than just as a 'box-ticking' exercise.'*

That is exactly how GDPR works now. The word 'appropriate' appears throughout the GDPR in qualifying the measures to be put in place to comply and satisfy accountability. This is already recognised by the ICO:

> *'Accountability is **not about ticking boxes**. While there are some accountability measures that you must take, such as conducting a data protection impact assessment for high-risk processing, there isn't a 'one size fits all' approach.*
>
> *You will need to consider your organisation and what you are doing with personal data in order to manage personal data risks appropriately. As a general rule, the greater the risk, the more robust and comprehensive the measures in place should be.'*

And, as the ICO confirms:

> *'To achieve this, if you are a larger organisation you may choose to put in place a privacy management framework. This can help you create a culture of commitment to data protection, by embedding systematic and demonstrable compliance across your organisation. Amongst other things, your framework should include:*
>
> - *robust program controls informed by the requirements of the UK GDPR;*
> - *appropriate reporting structures; and*
> - *assessment and evaluation procedures.*
>
> *If you are a smaller organisation you will most likely benefit from a smaller scale approach to accountability. Amongst other things you should:*
>
> - *ensure a good level of understanding and awareness of data protection amongst your staff;*
> - *implement comprehensive but proportionate policies and procedures for handling personal data; and*
> - *keep records of what you do and why.'*

Appropriateness under GDPR already ensures the flexibility the proposals discuss. As the UK government and UK ICO recognised previously, as above. It is therefore hard to see this proposal as anything other than prioritising business imperatives over data protection for the benefit of individuals.

The UK ICO's Accountability Framework is a good piece of work but is not a light effort for businesses - and is quite literally a box ticking exercise. But the key point is that, whatever requirement one puts on organisations, whether it is a box-ticking exercise or not has little to do with the standard or law and all to do with the culture of the organisation.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.2.1: Somewhat agree, in that the proposal on breach notification wording is good (the current wording in GDPR is hard to understand) and I believe that the role of DPO is greatly misunderstood - most I encounter are conflicted and many are not needed under GDPR - and the independence requirement for DPOs makes the position unworkable in practice.

However, the proposals describe GDPR. GDPR does indeed, through the Accountability Principle and related Articles, require a Privacy Framework to be put in place. The consultation paper could almost be describing GDPR. Therefore changes should be minor.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.2.2: Strongly agree, but this is the case already, so I see no change needed in the law. Keepabl provides Privacy Management SaaS and I can attest to the increasing demand among organisations to replace spreadsheets with automated SaaS solutions that help implement and manage a Privacy Framework that is often in place to various degrees albeit very manual.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.2.3: Strongly agree, but as above this is the case already, so I see no change needed in the law.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.2.4: Strongly disagree. Most private organisations do not need a DPO. However, DPO has become shorthand for Privacy expert and DPO-as-a-Service shorthand for Privacy consultant. In my view most are conflicted, either through their in-house role or through their duties. The role is hugely misunderstood. I propose simply removing the independence requirement as the momentum behind the various positions is going to be hard to change.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.2.5: Neither agree nor disagree. See my response to Q2.2.4. Organisations should have a Privacy Champion. They don't need to operate with independence.

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

RB response Q2.2.6: They won't maintain a role with the rights and obligations on both the organisation and DPO. However, they will have a commercial Privacy Champion - we see this already.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.2.7: Strongly agree.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.2.8: Somewhat disagree. One cannot identify risk (as the Proposals say they must do) without an assessment (which the Proposals also say they must do).

Such assessment should be appropriate to the risk. In my experience, in practice for most organisations, few processing activities present high risk and those that do (mostly around finance and health data) are heavily secured already. GDPR's risk assessment procedures are risk-based and DPIAs are only for likely high risk activities, of which there are few in practice and proportion in typical organisations.

Q. 2.2.9 Please share your views on why few organisations approach the ICO for 'prior consultation' under Article 36 (1)-(3). As a reminder Article 36 (1)-(3) requires that, where an organisation has identified a high risk that cannot be mitigated, it must consult the ICO before starting the processing.

RB response Q2.2.9: First, organisations do not want to approach the ICO voluntarily and potentially expose themselves to investigation. Second, there are few high risk processes for most organisations. Third, organisations are adept at managing risk, historically through Security but increasingly through Data Protection measures. Fourth, bad actors will always continue.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.2.10: Strongly disagree for the same reasons as in my response to 2.2.9.

Q.2.2.11. To what extent do you agree with the proposal to reduce the burden on organisations by removing the record keeping requirements under Article 30?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.2.11: Strongly disagree. As above, the Proposals mix up the order of priority in suggesting Privacy notices under Arts 13 and 14 are a duplicative process. One cannot create Privacy notices if one hasn't inventoried the activities and the lifecycle of the personal data - which you also stress is a key part of any privacy management program. The Art 30s are simply the tip of the iceberg, where the iceberg is the organisation's full personal data inventory - which, analogous to the Information Asset Register and other registers for Security, is the fundamental part of any Privacy program. People will simply ask to see the inventory if Art 30 is removed. No need for any change.

Q.2.2.12. To what extent do you agree with the proposal to reduce burdens on organisations by adjusting the threshold for notifying personal data breaches to the ICO under Article 33?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.2.12: Somewhat agree. The risk level justifying notification to regulators is very poorly drafted in Article 33. Indeed risk is dealt with badly in GDPR (and the UK ICO's recent transfer consultation documents).

Risk is well understood in Security as being a combination of likelihood and impact. 'Likely high' means likelihood - likelihood - impact. Risks are low, medium and high (or however many levels one assigns), not likely high. And references by the ICO to harm and damage instead of risk lead to further confusion. Harm and damage are analogous to impact, which is one part of risk calculations.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.2.13: Somewhat agree. However, this pretty well happens now anyway in practice. The UK ICO hardly issues enforcement outside of PECR. Indeed, the ICO should be able to set aside any such scheme and issue fines if appropriate.

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.

Q.2.2.15. What, if any, safeguards should be put in place to mitigate any possible risks to data protection standards as a result of implementing a more flexible and risk-based approach to accountability through a privacy management programme?

RB response Q2.2.14 and 2.2.15: My position is as above. There is no need to change the Privacy Framework aspects of GDPR, however I believe that certain aspects of the DPO and Breach notification could be improved as above.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.2.16: Strongly disagree. Indeed, I believe the question shows a lack of understanding of how Privacy compliance works in practice.

Q.2.2.17. To what extent do you agree that the proposal to amend the breach reporting requirement could be implemented without the implementation of the privacy management programme?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.2.17: Strongly agree.

Q.2.2.18. To what extent do you agree with the proposal to remove the requirement for all public authorities to appoint a data protection officer?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.2.18: neither agree nor disagree as I believe the independence aspect should be removed. This will make the role much better understood - and complied with - and lead to more DPOs being appointed.

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

RB response Q2.3.1: In my experience in the market, DSARs are very binary: organisations either get them or they don't. Those that get them tend to get 20 to 30 a month. Those that don't perhaps receive one a year from a disgruntled employee. Those who receive more than 30 a month are rare and tend to be larger organisations.

DSARs can be very expensive and time consuming to complete - again depending on the organisation and type of request. A good system can reduce the cost greatly. As an example, in the case of Deer v Oxford, [2017] 3 WLR 811, a relatively circumscribed, additional, DSAR process ordered by the court cost £116,116 and resulted in over 500,000 emails and documents being initially identified yet only 33 new disclosures.

However, all those I have spoken to who deal with DSARs fully respect the individual's right to make them and mostly lament the difficulty of finding the right tools at the right price to help them execute the DSAR, not the legalities around the process.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.3.2: Somewhat disagree.

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 agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.3.3: Strongly disagree. The cost isn't the issue as it's generally far higher than what people can afford to pay and introducing a set of rules with exceptions as the proposals suggest would only add to the complexity.

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 agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.3.3: Strongly disagree. It's a pointless admin task that doesn't impact the real price.

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'?

RB response Q2.4.1: The CNIL description in the Consultation appears appropriate.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.4.2: Somewhat agree if the removal only concerns those falling within the description of CNIL's view in the Consultation. No identification of individuals - or rather creation and retention of such data - should be possible without consent.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.4.3: Strongly disagree. These would only be acceptable when falling under strictly necessary, eg if a website visitor clicked to play a video.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.4.4: Strongly disagree. I couldn't disagree more strongly. This goes against the government's stated desire to protect individuals.

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?

RB response Q2.4.5: Possibly but I struggle to see how.

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?

RB response Q2.4.6: Technology is not anywhere near enabling this, particularly given the omnichannel way that such technologies can be used.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.4.9: Somewhat agree. Provided the rules are the same and opt-outs are in each communication, and honoured.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.4.16: Strongly agree.

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

RB response Q2.5.1: Strongly agree. There is a significant lack of trust in political parties and their practices, not least due to the activities of the Leave campaign and the Cambridge Analytica infringements. If not covered by PECR, the impact on individuals would be significant and likely grow over time.

Q2.5.2. If you think political campaigning purposes should be covered by direct marketing rules, to what extent do you agree with the proposal to extend the soft opt-in to communications from political parties?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Q2.5.3. To what extent do you agree that the soft opt-in should be extended to other political entities, such as candidates and third-party campaign groups registered with the Electoral Commission? See paragraph 208 for description of the soft opt-in

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.5.2 and 2.5.3: Somewhat agree. Provided the rules including on opt-outs are the same.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q2.5.4: Strongly disagree. They may impede it but that is why they are there.

Chapter 3 - Boosting trade and reducing barriers to data flows

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q3.2.1: Neither agree nor disagree. This has to be part of adequacy determinations, as does the review of legislation and rights and remedies for data subjects. As noted in paragraph 263: '*What matters most is whether a transfer mechanism provides the appropriate levels of protection for individuals.*'

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?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q3.2.2: Strongly agree, though this is not a point that is contrary to current practices. I believe this is available already, for example the Privacy Shield was a framework of a different nature. And the UK/EU can make such a decision by way of treaty as it did with the EU-UK TCA.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q3.2.3: Somewhat agree. There has to be an auditable method on ongoing monitoring before removing the 4-yearly reviews.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q3.2.4: Somewhat disagree. There should be an escalation route from administrative to judicial.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

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?

RB response Q3.3.1 and 3.3.2: Somewhat agree. This is a delicate balance. The Consutlation's text above this question suggests that the range of measures is insufficient. While any measure to make operationalising compliance easier for organisations is to be welcomed, I do not fully agree that that is an issue for commercial organisations - there was no issue with transfers in practice before the *Schrems II* case confirmed the obligation on data exporters to review surveillance laws etc in third countries. (Max Schrems would no doubt say this was largely because of the lip service paid to obligations in SCCs.)

On 3.3.2, a very positive and helpful resource would be to lead or support an international attempt to create a register that organisations could rely on for the TIA process, perhaps led by a body such as the ICC. If that could be done with the EU/EC, even better.

On a side note, I recommend sticking with established terms such as SCCs and TIAs. The names could be the UK Transfer SCCs, UK Processor SCCs (if the UK is creating those too) and UK TIA.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q3.3.3: Strongly agree provided this does not apply to any personal data that has augmented the data received into the UK.

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?

- *Strongly agree*
- Somewhat agree
- Neither agree nor disagree
- Somewhat disagree
- Strongly disagree

RB response Q3.3.4: Strongly disagree. The UK is not in the same place as New Zealand or other third countries with adequacy decisions - we already have GDPR as our law and this would be moving away from GDPR, which is contrary to the direction of global data protection laws. Having a flexible set of Transfer SCCs (which the EU ones are - or at least

could be if they're also applied to any transfer where Art 3(2) applies) means confidence for businesses and their customers. It's akin to having Cyber Essentials or Cyber Essentials Plus - the independent certification makes vendor due diligence easier.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q3.4.1: Neither agree nor disagree. I believe this is no different to the current situation. Standards setting out Privacy management programmes (often called PIMS in standards) are already out there and in the queue to be officially recognised.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q3.4.2 and 3.4.3: Neither agree nor disagree. I find it hard not to answer with 'you mean, like allowing use of the CE mark?' Recognition of any standard is good for organisations to be able to choose from a wide range of methods to better demonstrate compliance.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q3.5.1: Somewhat agree provided appropriate safeguards are in place based on the derogations. However, I believe this can be done with regulatory guidance since the Recitials an EDPB guidance are not binding law.

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

RB response Q3.6.3: Confirm a transfer is any exposure of personal data to a third country including actual transfer or making available, with exceptions for example for encrypted transit. Adopt the EU Transfer SCCs with a 1-page addendum for transfers. This will give certainty on transfers and certainty on the adequacy decision in favour of the UK, which is desperately sought by UK business.

Chapter 4 - Delivering better public services

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q4.2.1: Strongly agree provided this means joined-up services for businesses, in the same manner as the joined-up services for individuals in your examples, not allowing sharing personal data from the public sector with businesses, which is a far broader and more difficult issue, as the recent mis-handled General Practice Data for Planning and Research (GPDPR) programme. Keepabl's analysis of sharing personal data from the NHS and the Caldicott reports, highlights the public's willingness to support the NHS and NHS use of their health data, but their reticence to share their NHS data with private entities.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

Please explain your answer, providing supporting evidence where possible.

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

RB response Q4.3.1 and 4.3.2: Strongly agree provided safeguards such as those in the Consultation above these questions, on no re-use etc, are put in place.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q4.3.3: Strongly disagree. Only Article 9(2)(h) is subject to Article 9(3)'s requirement on relevant health professionals. Articles 9(2)(g) and 9(2)(i) present valid alternative grounds in that situation, particularly 9(2)(g) as there have been many temporary laws passed during the Covid emergency periods.

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?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q4.4.1: Strongly agree. This is a significant burden, which is justified in the limited circumstances listed.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q4.4.4: Neither agree nor disagree. The interplay between Article 6 and Article 9 requires significant review. I acknowledge the difficulty in matching Article 6 and Article 9, particularly for private sector organisations. A review of the Articles is a preferred route, rather than attempting to legislate all possibilities.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q4.4.5: Somewhat disagree. 'Public interest' is a well-rehearsed theme in English law.

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q4.4.6: Neither agree nor disagree. The definition of public interest is well-rehearsed. The definition of 'substantial' can be assisted in guidance (and case law).

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q4.4.8: Strongly agree. Though I believe the clarification is likely to restrict rather than expand relevant practices.

Chapter 5 - Reform of the Information Commissioner's Office

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

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

Q5.2.2. To what extent do you agree with the proposal to introduce an overarching objective for the ICO with two components that relate to upholding data rights and encouraging trustworthy and responsible date use respectively?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q5.2.1 and 5.2.2: Neither agree nor disagree. The list of objectives in GDPR is fair and the very title of GDPR is made up of the two components in 5.2.2 so I see little benefit here.

Q5.2.4. To what extent do you agree with the proposal to introduce a new duty for the ICO to have regard to economic growth and innovation when discharging its functions?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q5.2.4: Neither agree nor disagree. As the Consultation notes, the suits to promote and support growth are already there. And these should not override the two objectives of GDPR, with the focus on protection of the rights and freedoms of individuals when their personal data is being processed.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q5.2.5: Strongly disagree. Competition is a domain unto itself, and should continue to be regulated by domain experts. As the Consultation notes, there is increasing collaboration between the regulators, which is to be encouraged.

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)?

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

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*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q5.2.6 and 5.2.8: Strongly agree.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q5.2.10: If the question is a trojan horse for increased surveillance, then Strongly disagree. However, if the question is simply enshrining an existing obligation under due process, then neither agree nor disagree.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q5.2.11: Strongly disagree. The other regulators mentioned (Ofcom, Ofgem and Ofwat) have competition aspects and regulate industries with near monopolies. The ICO does not. The ICO should continue to consider the interpretation, implementation and enforcement of data protection laws within the context of human rights, competition and consumer rights, to name a few fields of treaty, law and convention. It should not be a vessel for the government's priorities.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q5.2.12: Neither agree nor disagree.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q5.2.12: Strongly disagree. The ICO should continue to consider the interpretation, implementation and enforcement of data protection laws within the context of human rights, competition and consumer rights, to name a few fields of treaty, law and convention. It should not be a vessel for the government's priorities.

Q5.3.1. To what extent d*o you agree that the ICO would benefit from a new governance and leadership model, as set out above?*

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q5.3.1: Strongly agree for the reasons in the Consultation.

> *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 agree*
> - *Somewhat agree*
> - *Neither agree nor disagree*
> - *Somewhat disagree*
> - *Strongly disagree*

RB response Q5.5.3: Strongly disagree. The ICO should continue to consider the interpretation, implementation and enforcement of data protection laws within the context of human rights, competition and consumer rights, to name a few fields of treaty, law and convention. It should not be a vessel for the government's priorities nor should the government of the day be able to delay or squash publication of reports from an independent regulator, for hopefully obvious reasons.

> *Q5.6.3. To what extent do you agree with the proposal to require data controllers to have a simple and transparent complaints-handling process to deal with data subjects' complaints?*
>
> - *Strongly agree*
> - *Somewhat agree*
> - *Neither agree nor disagree*
> - *Somewhat disagree*
> - *Strongly disagree*

RB response Q5.6.3: Somewhat disagree. This is analogous to complaints procedures for CSPs etc which are there as there are a high number of complaints and a large asymmetry in the relationship. However, this feels heavy-handed for every controller when they rarely receive such complaints and the relationship is very different given the data subject rights and high fines in GDPR.

> *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*
> - *Somewhat agree*
> - *Neither agree nor disagree*
> - *Somewhat disagree*
> - *Strongly disagree*

RB response Q5.7.1: Somewhat agree. The question is whether the ICO uses its powers under GDPR to a sufficient extent. Most enforcement is around PECR.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q5.7.2: Somewhat disagree. An expert report can be helpful, however, I believe the better solution is for the ICo to have such experts within its staff so that the reports are created by the ICO itself. This will apply the ICO's existing rules to such reports and remove the interaction of a third party, presumably a private entity. Such matters are highly confidential and the status of such reports within FOI and other regimes should be carefully considered. However, publishing anonymised results on a periodic basis might (might) have positive effects on sharing best practice.

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?

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

RB response Q5.7.3 and 5.7.4: According to my answer to 5.7.2, the ICO should bear the cost.

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

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

- *Strongly agree*
- *Somewhat agree*
- *Neither agree nor disagree*
- *Somewhat disagree*
- *Strongly disagree*

RB response Q5.7.5 and 5.7.6: Somewhat agree, though only with appropriate protections for witnesses similar to those in other regulatory and criminal investigations, including representation.

> *Q5.7.9. To what extent do you agree with the proposal to require the ICO to set out to the relevant data controller(s) at the beginning of an investigation the anticipated timelines for phases of its investigation?*
> - *Strongly agree*
> - *Somewhat agree*
> - *Neither agree nor disagree*
> - *Somewhat disagree*
> - *Strongly disagree*

RB response Q5.7.9: Strongly agree.

> *Q5.8.1. To what extent do you agree that the oversight framework for the police's use of biometrics and overt surveillance, which currently includes the Biometrics Commissioner, the Surveillance Camera Commissioner and the ICO, could be simplified?*
> - *Strongly agree*
> - *Somewhat agree*
> - *Neither agree nor disagree*
> - *Somewhat disagree*
> - *Strongly disagree*

> *Q5.8.2. To what extent do you agree that the functions of the Biometrics Commissioner and the Surveillance Camera Commissioner should be absorbed under a single oversight function exercised by the ICO?*
> - *Strongly agree*
> - *Somewhat agree*
> - *Neither agree nor disagree*
> - *Somewhat disagree*
> - *Strongly disagree*

RB response Q5.8.1 and 5.8.2: Strongly agree.

I hope this has been helpful feedback and I sincerely hope the result of the Consultation will be to increase confidence and certainty both within and without the UK concerning the UK's approach to being a responsible, connected, global partner.

Robert Baugh
19 November 2021