10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

Data: a new direction

techUK's response to the Department for Digital, Culture, Media and Sport's consultation on the future of the UK's data protection system

November 2021

Contact: Sue Daley, Director of Tech and Innovation I Neil Ross, Head of Policy I Dani Dhiman, Policy Manager for Data
Email: Sue.daley@techuk.org I neil.ross@techuk.org I Dani.Dhiman@techuk.org

About techUK

techUK is a membership organisation launched in 2013 to champion the technology sector and prepare and empower the UK for what comes next, delivering a better future for people, society, the economy and the planet.

It is the UK's leading technology membership organisation, with more than 850 members spread across the UK. We are a network that enables our members to learn from each other and grow in a way which contributes to the country both socially and economically.

By working collaboratively with government and others, we provide expert guidance and insight for our members and stakeholders about how to prepare for the future, anticipate change and realise the positive potential of technology in a fast-moving world.

Contents of response:

Introduction: positioning the UK to lead a global debate on data

The Government's consultation, Data: a new direction presents an opportunity for the first major update of the UK's data protection system since the introduction of the Data Protection Bill in 2018.

Run under mission 2 of the National Data Strategy to achieve a 'pro-growth and trusted data regime' these proposals spark a timely conversation preceded by a period of immense technological, business, and social change, not least as a result of the COVID-19 pandemic. These changes have tested the limits of existing data protection frameworks, highlighting some of the shortcomings of the General Data Protection Regulation (GDPR) while also revealing opportunities for a pragmatic evolution of the legislation for the benefit of consumers, businesses, and wider society.

These pressures for change are not just found in the UK, they are global and governments around the world will be examining their own reforms to their data protection frameworks.

In this situation the UK has a unique position to lead the global debate. Having left the EU the UK inherits a data protection framework based on the GDPR which has become a globalised standard and whose principles have been widely adopted.

Like others the EU is also planning its own reforms to its data protection regime however experience from the creation of the regulation suggests that this will be a slow process and the UK therefore has an opportunity to lead the debate and set the pace as a global process of data protection reform begins.

Successfully steering this debate however means being attuned to the trajectory of global data protection policy and seeking to converge on common principles, as the UK sought to do in the recent G7 statement, *Roadmap for cooperation on data free flow with trust*[1]. It also means protecting key pathways for data flows such as data adequacy with the EU, the interoperability of standard contractual clauses and other alternative data transfer tools. It also means ensuring that whatever additional flexibilities the UK provides in its own domestic rules, organisations are permitted to continue using data management policies that are designed to comply with multiple different regimes, as long as these give similarly high levels of protection to personal data as the UK's domestic laws. This will help prevent increased regulatory burden through double compliance and align with the Government's objectives to created outcome orientated regulation.

Through the *Data: a new direction* consultation we believe the Government has put the UK in a strong position. By retaining the fundamental principles of the GDPR, which the UK informed when a member of the EU, but seeking to make practical changes to the regulation based on our expertise as a leading digital economy and experience of using data driven technologies to respond to the pandemic the UK has

[1] G7 Digital and technology – track 2, G7 Roadmap for cooperation on data free flow with trust, HM Government, 2021

an opportunity to make changes to its data protection framework that remove the grit from the GDPR to support growth and innovation while also empowering individuals and companies to create better more trusted processes for managing and protecting personal data.

If we can get this right, we will not just seize the opportunity to update our data protection system for the 2020s, but create an approach which underpins our wider ambitions for our tech sector. For example, by crafting an approach to data governance that helps the UK remain Europe's most attractive destination to start and scale tech companies, make the UK a hub for data driven research and provide the cornerstone legislation on data that will be foundational to our ambition to be a world leader in AI powered technologies.

Our response:

techUK represents 850 technology companies operating in the UK. For our members the use of data is core to their business models. This consultation is therefore of huge importance to our sector. However, we recognise that impacts of these reforms go more widely than the tech sector and that this consultation is just the beginning of a longer conversation to get these reforms right. Through our regular engagements with DCMS and work as co-chairs of the National Data Strategy Forum we look forward to continuing this discussion with Government and other business and civil society groups.

techUK has provided detailed responses to the majority of questions raised in this consultation, these can be summarised in three core principles that we believe should steer the UK's approach to reform of the data protection system:

Securing Innovation and Growth: the Government has proposed a number of common sense improvements to the data protection system that our members have long called for. These changes such as the clarification on the bases for data processing under the legitimate interest test, clarification of data processing for research purposes, training AI algorithms and allowing businesses to more easily cooperate with Government agencies where there is a clear public need to do so. By making these changes the Government can provide certainty and clarity to organisations as they seek to innovate with data and develop new digital services and AI powered tools.

Ensuring the UK's data protection system is trusted by individuals and organisations: enabling citizens to exercise their data rights as well ensuring that the UK's data protection system is seen globally as providing avenues for redress, backed by an independent regulator, is vital. High levels of consumer confidence in the system as well as maintaining a reputation as a high standard location for storing and processing personal data is vital for citizens to have confidence in digital services provided in the UK and for companies to compete for international contracts and investment. Through these reforms the Government's privacy management frameworks offer an opportunity for businesses to create more tailored and trusted approaches to managing personal data as well as lessening some of the more prescriptive burdens on smaller firms. However, these reforms will

rely heavily on clear guidance from the ICO and the Government will need to ensure that through these reforms the regulator is well resourced and its independence remains without question. For us this also means the Government does not proceed with some of the proposals in this consultation which could have negative impacts on citizens abilities to exercise their rights. For example, the reintroduction of a fee for subject access requests or the suggested proposal to remove Article 22 of the GDPR.

Making the UK a global hub for data: International data flows are the cornerstone of global businesses. Both UK headquartered and international companies operating in the UK regularly engage in data transfers with business partners across the globe. Flows of data is not just an issue for the tech sector, with the operations and supply chains of virtually every modern business supported by the transferring of personal data. Whether that is detailed data sets for complex digital services, or the financial and logistical information needed for the trade in goods or provision of services. To achieve the objectives of Mission 2 and secure 'pro-growth and trusted data regime' the UK needs to be seen as a trusted destination for data transfers. While adequacy decisions such as the UK adequacy decision from the EU helps reduce business burdens, its symbolic importance is arguably just as vital for allowing businesses and investors to make a strong case based on the continued alignment of high standards of data protection. Maintaining access to global data flows, such as through EU adequacy, as well as making pragmatic reforms to the data protection system is the most effective way to succeed in achieving Mission 2 of the National Data Strategy.

Chapter 1- Reducing barriers to responsible innovation:

1.2 – Research purposes

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

Strongly agree

Increasing clarification of the bases for data processing for research purposes is seen as one of the major prizes for boosting innovation in this consultation. By creating clearer definitions supported by easily understandable guidance and examples of how data can be used and re-used by researchers the Government has the opportunity to increase the attractiveness of doing research in the UK. Particularly if the Government can achieve clarity for researchers so that smaller companies and research groups feel confident to use data sources, reducing risk adversity, this will have significant benefits.

techUK supports the Government's objective to bring together research specific provisions, however in the feedback from our membership companies have highlighted the broad range of perspectives on what classifies as *research*. When drawing these provisions together we would urge the Government to consult not only with the academic community but also with industry to ensure the right provisions are bundled together.

It will also be vital that any guidance emerging from the above changes is clear, accessible and understandable to ensure the maximum use of the proposed reforms.

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

Creating a statutory definition will be important for clarity, however in doing so it is vital that this definition is broad to allow the regulator to clearly specific key activities that fall underneath it.

In our conversations members have raised a number of issues for the Government to consider as it seeks to draft a definition:

- It is not fully clear from the consultation what kind of research the Government is aiming to capture in a statutory definition of *scientific research*. techUK would suggest the Government uses this consultation to gather input

on what research purposes are best covered by a new definition and then seek to update legislation accordingly.

- There are questions around how the definition, will apply to social scientific research, which is more likely to use personal data, as well as research for the development of a new product which in the case of developing new technologies, medicines etc. is obviously *scientific*.

- It is important any definition should seek to reflect the contributions the private sector can make in advancing scientific research, particularly in light of COVID-19, where public and private partnerships have proven to be invaluable in supporting the UK's recovery from the pandemic. In many cases, our members have been able to use anonymised and aggregated data sets to gather insights to inform the decision-making of public authorities. Historically, anonymised data sets from the private sector have been vital in supporting scientific research and economic analysis to inform policymaking and their contributions should be considered when implementing reform.[2]

- The definition should seek to include research conducted for the research and development of products or services, including any inputs connected to this purpose. For example, activities that would be covered by the UK's R&D tax credit which is currently being expanded to cover cloud computing and data costs.

- The definition of 'scientific research' should focus on the activity and not seek to exclude organisations based on their type, i.e., public, private, profit or non-profit. All should be covered if they are undertaking legitimate scientific research.

- It is also important to note that while legislation provides clarity how that legislation is worded can have significant impacts on its interpretation if challenged in court as well as in any subsequent guidance by the regulator.

techUK would support a definition of *scientific* research that encapsulates both traditional scientific research in an academic or research settings and social scientific research.

We would suggest in any legislation the Government sets out clearly in explanatory notes the intention of the legislation to create a permissive environment for data processing where this is clearly for the intention of research in both the public and private sectors with the regulator then able to deliver effective guidance to support the policy objective.

Q1.2.3. Is the definition of scientific research currently provided by Recital 159 of the UK GDPR ('technological development and demonstration, fundamental research,

[2] Google: covid-19 community mobility reports, Future of Privacy Forum, 2021

applied research and privately funded research') a suitable basis for a statutory definition?

Yes

We believe recital 159 provides at least a suitable basis, however when drafting any legislation, we encourage the Government to take note of the points raised in response to questions 1.2.1 and 1.2.2.

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?

Somewhat Agree

Identifying the correct legal ground for research can be a complex process. Each legal ground can come with its own conditionality and opportunities that can shape the scope of research in terms of flexibility, and the extent to which the data processing must comply with data protection rights.

While feedback from our members indicate that the law is generally well understood with support of ICO advice and guidance. At times, there can be confusion between researchers and participants where legitimate interest is often the legal basis for research, but additional consent may be required to comply with interacting regulatory frameworks e.g. tort of confidentiality.

Members also highlight the tension that occurs when two organisations rely on different lawful bases for the same research purpose.

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

Neither agree nor disagree

techUK does not disagree with this approach, however we have some general concerns that should the Government allow university research projects to rely on (Article 6(1)(e) of the UK GDPR) as a lawful ground be permitted without also reforming the bases for processing personal data for research outside a university setting, this could distort the market in favour of university-based researchers.

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

Somewhat agree

techUK members would in principle welcome a new, separate lawful ground for research which supports not only academia, but the commercial sphere too. In the experience of our members, when partnering with academic institutions, members tend to own the datasets being used in the piece of research. An expanded lawful ground would clarify the extent to which organisations can and cannot share data with partnering research institutions.

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

Recommendations from members on possible safeguards include:

- Government taking into consideration existing guidelines and ethics for research,
- Non-repudiation controls to safeguard individuals' data as well as the organisation and its entire supply chain in the event of misuse,
- De-identification of personal data,
- A form of balancing test could be introduced
- Security safeguards as well as contractual ones e.g., commitments to confidentiality and prohibited steps to re-identify anonymised data sets.

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

Somewhat agree

techUK is supportive of this general right, however it will be vital that any reforms provide other bases for data processing beyond consent where thresholds are met and with suitable safeguards. This concern derives from the experience of our members where an overreliance on consent can lead to this basis being sought above all others. Any guidance relating to this should be clear that other legal bases are available if their conditions are met.

Such an approach would also better support the experiences and approaches our members take when conducting research, whereby end-goals may not always be clearly defined at the start of research and the valuable findings which contribute to their innovation develop unplanned and unexpectedly.

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

Strongly agree

If the Government takes forward the reform suggested in 1.2.8 then it should provide clarity further processing for research purposes is both (i) compatible with the original purpose and (ii) lawful under Article 6(1) of the UK GDPR.

Q1.2.10. To what extent do you agree with the proposals to disapply the current requirement for controllers who collected personal data directly from the data subject to provide further information to the data subject prior to any further processing, but only where that further processing is for a research purpose and it where it would require a disproportionate effort to do so?

Somewhat agree

Whilst techUK is supportive of this proposal in principle, our members would welcome further clarification on what "disproportionate efforts" would mean in practice. Guidance from the regulator will be vital to set out the operationalisation of this definition with clear criteria to ensure it is not misinterpreted or misused.

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

It should remain good practice to update data subjects and/or provide publicly accessible notices on how data collected for a specific research project is being reused.

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?

Strongly Agree

The Government's proposal to allow organisations to re-use personal data for a purpose different from that for which it was collected are favourable in terms of alleviating burdens on businesses where clear conditions are met and supporting innovation in data use.

Further processing may enable organisations, for example, to use personal data for research purposes, if such purpose meets the safeguards of an important public interest test.

Such reforms could also help organisations to come up with innovative solutions that are not only beneficial for their businesses but also for society at large. For example, there is a benefit in these reforms with regard to the with the wider goal of

Government to boost and support of Privacy Enhancing Technologies (PETs) and the use of machine learning for safety or integrity purposes.

While there is a clear case for repurposing of data under Article 6(4) of the UK GDPR, it is important that the government makes a clear distinction between further processing and new processing to avoid any kind of ambiguity in relation to use/re-use of personal data. This will help business be certain of the activities they are taking, vital to achieving the Government's aims of supporting an increase of further processing under specific circumstances and ensuring citizens understand where data may be reused.

Scenario based guidance could also help the Government achieve its aims here.

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

The levels of uncertainty for the use of article 6(4) will vary between businesses of different sizes, and engaged in different processing activities. Providing increased clarification with an appropriate level of discretion for businesses and guidance from the regulator that supports repurposing in certain circumstances will help address some of the imbalance between businesses of different sizes, sectors and experience. Helping this type of data processing to become more accessible which we believe will have general benefits for the UK economy.

However, techUK and its members would welcome further clarity on how public interest will be defined; a vague definition may lead to increased legal uncertainty for data controllers, and a lack of understanding on how data is being processed for data subjects.

To remove any ambiguity, the ICO should develop of a set of principles or considerations that must be fulfilled to demonstrate that further processing will in fact support the public interest. Such an approach would give organisations further legal certainty, consequently removing a barrier to innovation while also providing detail to citizens on where data may be reused.

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?

Somewhat agree

techUK is supportive of this approach, provided there are sufficient safeguards and clear transparency requirements for businesses to inform data subjects when data

is passed on to a different controller. Businesses will seek a high degree of certainty before undertaking further processing by a controller different from the original and therefore such a reform will need to be supported by clear guidance.

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

Somewhat agree

techUK is supportive of this approach as it will be important to provide clarification as businesses will seek a high degree of certainty to enable further processing, particularly where consent was given for the original purpose. Clarification will also assist business to be able to explain with more certainty and security to data subjects how their data has been further processed, without re-seeking consent in the event of a subject data access request.

There is a risk that without clarification on this point to allow businesses to robustly defend the legal basis for reprocessing that companies will simply not do so to avoid any legal risk.

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

techUK and our members strongly support this approach with this type of reform having been long advocated for by our membership.

Getting this reform right has the potential to take significant strides towards modernising the UK's data protection framework allowing data to be processed for common sense purposes in a way that any reasonable consumer would expect, such as reporting criminal activity or improving a network's security.

Doing so will also have the benefit of reducing burdens on businesses and improving the environment for developing AI applications in the UK.

In implementing the list, the Government will need to achieve two objectives, (i) provide clarity around the specific functions covered, supported by clear guidance from the ICO to ensure the provisions are not abused, (ii) and ensure that there is a mechanism to update this list as technology and public expectations evolve.

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 believe that the list provided offers good start with coverage of public service duties as well as routine business operations purposes such as securing a network, digital advertising measurement or seeking to correct bias in an AI system.

There are some purposes missing from this list that techUK members would welcome being added, or clarified as being in scope under the existing proposals.

We have provided some suggestions below which we believe are in the spirit of the Government's approach to updating the list. These additions include:

- Allowing for data to be processed in efforts to prevent and detect fraud (this could be included under *f) Improving the safety of a product or service that the organisation provides or delivers*),
- Allowing the processing of personal data to better customise the functionality of services based on the preferences of users, this could be added under *h) business innovation purposes aimed at improving services for customers,*
- The ability to de-identify personal data through pseudonymisation or anonymisation, for example for aggregated statistics and reports,
- Allowing the processing of personal data for workplace equality assessments (this could be under, *h. for internal research purposes),*
- For maintaining physical security of premises and other land (this could be under *f) improving the safety of a product or service that the organisation providers or delivers),*
- 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*).

Further detail would also be appreciated on how the Government intends to monitor the construction of this list and any criteria Government is examining for the addition of further processing purposes.

The logic for creating the list is to update the UK's data protection framework as technology and the expectations of how businesses use data has evolved. It is therefore important that Government considers ways in which to keep this list up to date to keep pace with further technological innovation.

We would also like to highlight some further considerations for Government raised by our membership in response to this question:

- It will be important to guard against a perception that developing legitimate interest processing can only be used for the purposes in the exhaustive list and that inclusion on the exhaustive list just means that a legitimate interest is deemed to exist without the need for a balancing test. The continued availability of the legitimate interest – supported by a balancing test remains an important part of the data protection system and we would not like to see this system underutilised as result of this welcome innovation. This is

particularly true for those members who will still be required to follow EU rules around legitimate interest.

- To support the utility of the suggested list, we would also welcome clarification around how the proposed list would work alongside the right to object under Article 21(1) of the UK GDPR, in particular whether the listed activities could create a prima facie rebuttal to the right.

- The Government should provide clarity on the interaction between this new exhaustive list and Article 21 of the GDPR, *Right to Object* and whether consumers would still be able to exercise this right in light of this proposed exhaustive list. techUK believes this right should still remain exercisable even under the exhaustive list.

- We would also encourage the Government to take an industry-specific approach when developing the list in order to identify how it may interact with existing regulation eg. Privacy and Electronic Communications Regulations (PECR). This consideration is especially important in cases where interaction between the list and existing regulation may unfairly impact particular industries by way of stifling innovation or opportunity.

- Members have voiced support for maintaining the definition included in recital 49 of the GDPR in relation to the suggested exhaustive list activity e) Improving or reviewing an organisation's system or network security. Doing so will allow interoperability between the UK's exhaustive list and where legitimate interest balancing tests have been conducted in other jurisdictions. This will make it easier for businesses to secure their network, particularly when it covers multiple jurisdictions.

- The Government should examine where other jurisdictions change their definitions of legitimate interest, for example in the revised EU Network & Information Systems Directive (NIS2). There is a strong argument to align these definitions in practical cases such as this to reduce burdens on businesses.

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

Guidance and examples from the regulator around more 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.

Any guidance however should seek to encompass the wide range of processing needs that would appear under items h) and f). This could be effectively informed by a principles-based approach by the regulator with examples used to provide case studies.

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?

Neither agree nor disagree

There are some obvious examples from the Government's proposed list such as, *a. Reporting of criminal acts or safeguarding concerns to appropriate authorities*, *b. Delivering statutory public communications and public health and safety messages by non-public bodies* and *e. Improving or reviewing an organisation's system or network security* where the legitimate interest balancing test for children's data should not be needed.

In these areas the data subject's age has little to no bearing on the underlying processing activities. As such, it would prove burdensome from a compliance perspective to draw an additional distinction based on the age of the data subject, and for some companies and operations defeat the purpose of the exhaustive list these activities for adults' data only.

However, this is less clear in in the other options given cases where a legitimate interest balancing test should remain.

If the Government decides to apply a balancing test to part of the list for children's data techUK and our members would welcome clarity on whether any balancing test applicable to the proposed exhaustive list would also require the 'extra weight' for legitimate interest tests under the ICO's Children's Code. Our view is that whatever the Government's decision the strength of these tests should be consistent to reduce the burden on businesses.

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

techUK welcomes the government's detailed exploration of the role of fairness in data regulation and the recognition that this is closely connected to the risks of AI technologies in amplifying existing societal inequalities. The data used for the development and use of AI technologies can impact people's lives, and fairness is therefore an essential consideration in data regulation.

It is important that the outcome of data reforms aligns with the government's forthcoming White Paper on AI Governance, to give the tech industry as much clarity as possible on legal obligations with regards to fairness. The ICO's Guidance on AI

and Data Protection[3] provides a useful overview of how data protection legislation applies to AI, and the Bridges v South Wales Police judgment provided an example of the application of the UK Equality Act 2010 on public sector use of AI-powered technologies.

These have gone some way to make legal obligations clearer, yet further clarifying steps would be welcome.

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

For AI technologies to be deployed both effectively and responsibly, both suppliers and adopters must understand their responsibilities to ensure fairness.

We agree with the government that defining fairness is complex, and greater clarity on its scope and substance in the data protection regime as applied to the development and deployment of AI systems would be welcome. However instead of trying to make an AI system completely 'fair', a more realistic goal should be to detect and mitigate fairness-related harms as much as possible. Further guidance in this area would help deliver better outcomes for individuals and organisations.

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?

As AI technologies become ubiquitous across the economy, including in the delivery of public services, a wide range of legislative regimes and regulators will play a role in the substantive assessment of fairness of outcomes directed by AI technologies. This is necessary as different sectors require expert regulators who can assess fairness in context.

It is, however, increasingly important that these regulators work collaboratively to give reassurance that the impact of AI on every sector is appropriately considered and that organisations can be confident in accessing guidance on fairness which is accurate and applies to them. There is an important role here for the Digital Regulation Cooperation Forum (DRCF).

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

[3] https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/

It is important for long-term trustworthiness that there are safeguards in place to prevent the use of data and data-driven technologies to drive unfair outcomes. techUK agrees with the Government that such safeguards are currently spread across a number of different overlapping regulations and regulators. This can cause confusion, and the Government's proposal to clarify organisations' responsibilities with regards to fairness, in the forthcoming AI Governance White Paper is therefore welcome.

The risk of developing a substantive concept of outcome fairness in the data protection regime is that it could become overly prescriptive. Fairness can be subjective and is often defined differently across different contexts. These different definitions can be incompatible, for example, there are very different issues around fairness for self-driving cars compared to forecasting supply chains, though both may use the same AI/machine learning techniques.

A concept of outcome fairness embedded in data regulation is unlikely to account for all such different scenarios and would therefore need to be supplemented by other definitions regardless. It may therefore be better for the ICO to work with other bodies to ensure AI is accounted for in the assessment of the fairness of outcomes across regulatory areas, and for ICO's responsibility to focus mainly on fair data use and procedural fairness.

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

Somewhat agree

techUK supports efforts to increase the legal certainty and clarify the bases around which organisations can use personal data for the purpose of training and testing AI responsibly, while appropriately balancing safeguards that take into consideration the costs of compliance.

Tackling AI bias and creating thoroughly tested products is fundamentally important to the health of the ecosystem in the UK. The UK also has the opportunity to further enhance its position as a development hub for AI technologies should the data protection system provide confidence to companies to access a wide range of data (subject to appropriate safeguards), for training and testing of AI products.

For example, natural language processing models with large numbers of parameters, more data, and more training time acquire a richer, more nuanced understanding of language. Natural language processing (NLP) solutions can help organizations turn unstructured data into insights and make information easy for customers and knowledge workers to access and understand, improving knowledge worker efficiency, boosting business growth. By making the UK a more attractive place to

develop and deploy NLP models and solutions, this would have significant benefits for the UK tech sector and wider economy.[4]

In addition, a common misconception is that omitting special categories of personal data, such as gender, age or ethnic origin, would ensure AI systems do not discriminate. However, sometimes biases can only be corrected when input data includes these special categories. We therefore support the Government's plan to include the processing of personal data and sensitive personal data for the purpose of bias monitoring, detection and correction in relation to AI systems, subject to appropriate safegaurds, as part of an exhaustive list of legitimate interests that organisations can use personal data for without applying the balancing test.

However, to support compliance with other countries extra territorial data protection frameworks the Government and the regulator should consider how to best provide guidance to around how to support UK based businesses to compliantly use data sourced from multiple jurisdictions to train AI systems.

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

Feedback from our members indicates mixed experiences in following a legitimate interest assessment for the development of AI systems. Whilst some members are able to proceed with development and deployment of AI subject to appropriate safeguards, others are challenged by the legal uncertainty around the balancing test and the concept of fairness, meaning it is often considered risky to solely rely on legitimate interest.

One member flagged limitations in other regulation for example, the Privacy and Electronic Communications Regulation (EC Directive) 2003 (PECR) on the processing of network metadata which does restrict the ability to unlock the value of data they already have a legal basis to process to develop better customer supporting solutions.

In questions 1.5.6-1.59, members encourage Government to consider the distinction between the "development" and "deployment" of AI when implementing reforms. In the experience of some of our members, personal data collection and processing in these cases may vastly differ in terms of quantity of data, purpose and categories and therefore be subject to different data protection requirements.

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

In the experience of our members, legitimate interests offers only a narrow set of freedom to collect data once the balancing test has been applied. Due to re-use

[4] NVIDIA, Using DeepSpeed and Megatron to Train Megatron-Turing NLG 530B, the World's Largest and Most Powerful Generative Language Model, 2021

limitations, data based on consent such as cookie data and network metadata is unusable.

In such cases, where additional consent must be acquired before re-use, the relationship between data controller and processor can easily become confused. This means that changes/expansions to data use can easily be overlooked or ill-considered.

Members would also welcome clarification on whether re-use limitations apply to the data, model or "inferred data" extracted from the models that have been previously constructed (in the context of research).

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

In the experience of our members, this can pose a challenge as it can be challenging for researchers in the field of AI to fully understand the legislation. The cost of ensuring compliance can be particularly burdensome for organisations. It is not always a straightforward process to identify the legal base to process data for the purpose of research.

Please see our earlier answers to section 1.2 for further details.

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

In the experience of our members, the transition from research to commercialisation is unclear. With AI technologies, data can be transformed and encoded in AI models – legislation does not specify the process for the handling of encoded data, their reuse rules and migration from research to commercialisation.

Please see our earlier answers to section 1.2 for further details.

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

Somewhat agree

Processing sensitive personal data can be immensely useful for the purpose of bias monitoring, detection and correction in relation to AI systems. We support 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. Producing an exhaustive list is one option for providing clarity in a number of circumstances.

However, the Government may wish to examine whether it should create a clear legal basis for using this type of data (with examples as reference). Such an approach may be more implementable and future-proof.

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

Please see our answer to 1.5.5 and 1.5.10.

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

A new condition tailored to the purposes of bias monitoring, detection or correction would provide greater clarity on the types of sensitive personal data that can be processed.

Please also see our answer to 1.5.5 and 1.5.10.

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

The Government will need to include accountability safeguards and measures to ensure the data is not being used for purposes beyond bias identification and mitigation.

Further in the experience of some of our members, many AI systems are developed using external providers who act mainly as data processors. Therefore, accountability requirements should apply equally to data controllers as well as processors.

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

Somewhat agree

techUK supports the Government's position on clarifying the threshold at which point an automated decision may be subject to human review to one which relates to a solely automated decision which produces legal or similarly significant effects.

Automated decision making does not solely relate to the use of AI, with an automated decision being made through simple algorithms, data analysis or scoring systems used in automated forms or surveys. The prevalence of such approaches has increased dramatically and as a result to create a more relevant and targeted regime of redress for data subjects we support the Government's proposal to raise and clarify the threshold at which an automated decision can be reviewed.

While there is limited case law in the UK such an approach would follow the trajectory of similar jurisdictions such as in the Netherlands where rulings in the Amsterdam District Court have sought to clarify the thresholds around 'solely' automated decisions and the impact of the effects on data subjects.

Government should apply a similarly high threshold to the meaning of "legal or similarly significant effects." There are many examples of automated decision making which have no legal effects on a user e.g., personalisation of retail offers or advertising to consumers.

techUK believes any clarification should be broad and principles based allowing the regulator to provide further detail in guidance.

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 disagree

As set out in our answer to Q 1.5.14 techUK supports the Government's view to clarify article 22.

Q1.5.17. To what extent do you agree with the Taskforce on Innovation, Growth and Regulatory Reform's recommendation that Article 22 of UK GDPR should be removed and solely automated decision making permitted where it meets a lawful ground in Article 6(1) (and Article 9-10 (as supplemented by Schedule 1 to the Data Protection Act 2018) where relevant) and subject to compliance with the rest of the data protection legislation?

Strongly disagree

techUK has not detected in our membership or among wider stakeholders a desire to remove article 22.

Article 22 is an important protection for citizens, and we also have concerns that the removal of Article 22 would put the UK out of step with global approaches to redress of automated decision making.

Ensuring equivalence of outcomes is vital to reassuring international partners that personal data can be processed in the UK through equivalence decisions such as adequacy or without the coverage of stringent contractual clauses.

Removing Article 22 and moving against a global trend toward enabling redress for certain automated decisions could see other jurisdictions a) seek to prevent their citizens data from being used in the use of and development of automated systems such as AI and machine learning in the UK, b) their regulators may issue guidance around contractual clauses which makes this process difficult.

Many companies do not hold nationality data and therefore would find it extremely difficult to split data sets if third country legislation or regulator guidance made it risky to process their citizens data in the use of AI tools. Members have therefore raised concerns that if article 22 is removed it could increase compliance burdens for UK firms seeking to process international data and have negative impacts of the development and use of automated services as well as AI and machine learning technologies.

The removal of Article 22 would also disenfranchise citizens in their ability to challenge or seek further information on automated decision-making that has a significant impact on them, including any unexpected outcomes which may occur in the development of AI technologies.

As a result, we do not see a strong argument for the removal of Article 22 but do support clarification as outlined in our response to 1.5.14.

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.

Government should consider any amendment to Article 22 in the light of conclusions to the CMA's market study on digital advertising and online platforms that the design and implementation of GDPR – namely the stipulation of consent as the only available legal base for activities relying on profiling – has advantaged some business models over others and has impacted competition in certain markets.

The Government should review this and aim to ensure that any amendments should not create further barriers to competition.

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).

Here, members would encourage Government to draw a distinction between automated decisions and AI – the former will be a static formula and should be published or made available upon request. The latter, should explain in clear, easy to understand language the basis for the use of AI, including steps taken to exclude/mitigate unconscious bias.

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.

Yes, the data protection legislative framework is a good starting point for evaluating any data-driven harms related to AI. In addition, higher-risk AI use cases should be evaluated through a sector-specific regulatory lens. In many sectors it will be the sector experts who are best able to judge the risks associated with introducing specific AI technology. Focusing on context and specific applications will be key to ensuring the UK's response to the adoption and use of AI is proportionate, pro-innovation and practical.

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?

Neither agree nor disagree

Feedback from our members indicate that regulatory guidance is the more appropriate mechanism for clarifying when data is anonymous. Clarification of the test for anonymisation is seen as highly desirable for our members..

Members would also ask the Government work with the ICO to take the following into the consideration when implementing any reforms:

- Organisations should have flexibility to evolve approaches to anonymisation as they continue to innovate and as technology develops.
- Concrete guidance in terms of which steps to follow to anonymise data would be a good starting point to give more flexibility to organizations to anonymise data sets, provided that such guidance is not overly prescriptive and technologically neutral.
- Members have also raised an increasing reliance on pseudonymised data, particularly for use in AI systems. This raises questions as to whether the requirement for de-identification is still relevant and whether greater weight should be given to de-personalisation of data instead.

- If the Government does decide to make changes any proposed changes should ensure consistency between the forthcoming ICO guidance on anonymisation and the proposed text on anonymisation.

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

The majority of our members have pointed to recital 26 of the UK GDPR, which they believe would carry more weight than the explanatory report to Convention 108 of a non-binding guidance document.

However, while the majority have taken this view some members believe Convention 108 is the correct approach.

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

Since organisations will have different methods, systems, and processes in place for the re-identification of datasets, any test should be proportionate rather than absolute so as to not inhibit innovation. Risk of re-identification should be considered in light of different factors including, the overall size of the data set, the number of data subjects, the complexity of the anonymization techniques, access to other identifiers, etc.

Government should also take into consideration re-identification capabilities beyond the data controller and processor e.g. if data is leaked outside the organisation.

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

Yes, having government support privacy-enhancing technology would help promote the use of and reliance on technology to anonymize data sets, in particular given that many questions remain as to whether such technology can truly be employed to meet the legislation's anonymization threshold (e.g. tokenization).

1.7 Innovative data sharing solutions:

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

Yes

The role of the government would be to enact and ensure compliance with common standards. Such an approach could set out clear guidelines for the use of legitimate

interest as a lawful ground for processing, so it is clear for both data intermediaries and end customers when such a lawful ground will be appropriate.

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?

Having worked closely on the Open Banking initiative, we know that the free flow of data can bring benefits to consumers in certain markets and extending the principles of smart data is of great interest to our members.

With regards to accreditation, we agree that in markets where a smart data structure is appropriate and there is a strong rationale for tackling unnecessary burdens, accreditation should be operated across markets. Duplication of accreditation must be avoided to ensure third-party providers (TPPs) are not burdened with unnecessary cost and administration, and are able to work across different schemes.

It is essential that any processes/requirements vis-à-vis TPPs be in line, as is appropriate, with those of Open Banking. When considering any permission or authorisation procedures, thought should also be given to the regulation and oversight of non-UK and non-EU based TPPs and any extra territorial reach powers or restrictions. Government should take care that the setting of standards is an open and transparent process subject to broad market consultation, so that it does not inadvertently become a barrier to competition.

1.8 Further Questions

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?

Government should implement incentives to encourage organisations to process data for the purpose of achieving Environment Social and Governance (ESG) objectives.

Chapter 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'?

Strongly agree

techUK supports the Government's intention to make the accountability framework as set out in legislation less prescriptive, more flexible, and with a greater emphasis on the risk-based approach.

This would more closely align data protection law with its original policy goal, which was to ensure data controllers and processors take deliberative and thought through decisions about when and how to process personal data.

However, Government should also be mindful that too much flexibility in legislation could create uncertainty for organisations and create additional costs and burden. This aligns with the Government's wider reforms to the UK's approach to regulation that is being pursued across other aspects of digital regulation.

We also strongly support the Government's approach to allow international companies which set their compliance posture to fit the markets they operate in to continue to be able to utilise their existing privacy policies under the proposed new regime. Those members who have invested heavily in EU GDPR compliance should not need to make any changes in order to be compliant under the proposed reforms. Members would therefore caution the government against introducing changes that include elements which are duplicative or parallel to the existing framework. Such an approach risks over-burdening organisations operating across multiple jurisdictions with additional and/or differing compliance obligations.

This is an important addition which recognises the compliance positions that companies have to adopt based on their size and recognising the extra-territorial effects of data protection regimes around the world. This will also be useful for UK companies as they scale, allowing them to modify the proposed Privacy Management Programme (PMP) as they grow.

Government should explore the possibility that PMPs can be used in complex supply chains. The CMA has observed that participants in complex supply chains are disadvantaged by the compliance requirements of GDPR and this can put them at a competitive disadvantage relative to their vertically integrated competitors.

Members are broadly supportive of this approach including the Government's plans to introduce PMPs however questions remain over how risk will be assessed and the sequencing of the introduction of the legislation and issuing of guidance from the regulator for PMPs to be effectively used.

techUK would encourage the Government to work with the ICO to work on this sequencing and to set out clear guidelines for how companies can assess risk under the new framework. How companies can assess risk will need to involve clear and actionable principles on how organisation should go about assessing risk so that these can be enacted in a robust, defensible, and repeatable way.

It is particularly vital that the ICO guidance which underpins the new accountability framework and PMP framework embeds the core principles and redress features of the GDPR, which the Government says it wishes to retain. This will be important to ensuring that the PMP framework does not look like an international outlier, strikes the right balance between flexibility and allowing citizens to exercise their rights and ensures the UK is able to maintain important arrangements such as EU adequacy.

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

techUK supports this statement. As mentioned in the answer to 2.2.1 how companies can assess risk in a robust, defensible, and repeatable way across multiple jurisdictions (some of which apply a more prescriptive approach) will be foundational to the success of the PMP approach. Without this companies will default to tried and tested methods such as strict privacy policies. This would minimise any benefits from PMPs.

However, the Government should expect that some companies do not avail themselves of the extra flexibilities offered in the PMP framework should they have data management practices due to a need to align with other jurisdictions such as the EU GDPR. Ensuring such practices are still valid in the UK will be vital to reducing business burdens, ensuring international arrangements such as adequacy are maintained and allow companies to take different approaches to their data management practices depending on their size. To us this is the inherent benefit of the PMP approach and recognises the realities of the extra territorial aspects of data protection legislation.
For a PMP to really succeed however more clarity will need to be provided on the obligations thereof, otherwise this may be open to interpretation such as the current view of 'appropriate organisational and technical measures'. To do so, we believe there are strong benefits in the approach adopted by other regulatory bodies such as Ofcom, wherein they publish annual plans which help organisations better understand the strategic priorities of the regulator for a given year.

Any PMP requirements should also take into consideration interaction between industries and existing regulation eg. PECR.

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

PMPs offer the opportunity to put consumer demand and competitive pressures at the heart of the way data is treated. Consumers will demand high standards of data protection as well as innovative products. We believe the PMP approach has the ability to allow companies the ability to adjust their data management practices aligning with consumer demands.

However, the Government must ensure that changes will not create pathways for companies to dilute data protection standards or reduce the application of the core principles of the GDPR or decline of the UK's high data protection standards.

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?

Somewhat agree

We believe this reform will reduce the costs for smaller companies while also increasing the ownership of data management practices in house. However, it is vital that a named person within the organisation remains responsible for data protection.

From the feedback we have received we would expect most larger companies, companies that handle large volumes of data and those who trade internationally to still appoint a Data Protection Officer (DPO) due to the different data protection regimes they will need to comply with and the likely demands of their customers.

Members have raised concerns that, as drafted the Government's proposal would prevent organisations to allow an existing DPO to also monitor compliance with the PMP due to the independence they require for GDPR purposes. In such cases, organisations would have to appoint an additional professional to oversee its UK privacy management programme. This is not only inefficient and burdensome but offers little discernible benefit for organisations or data subjects in the UK. The Government should therefore seek to allow DPOs to also monitor compliance with the PMP.

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

As mentioned in our response to 2.2.5 from the feedback we have received we would expect most larger companies, companies that handle large volumes of data and those who trade internationally to still appoint a Data Protection Officer due to the different data protection regimes they will need to comply with. In such cases, any changes should not shoulder additional compliance burdens on these organisations.

It is important to allow companies operating in the UK to be flexible to meet both local and international obligations of which data protection officers are an important part.

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

Although data protection impact assessments (DPIAs) are a good way to tease out data protection risks, feedback from members indicate that the DPIA process can be a more prescriptive duplication of analysis performed by legal teams.

Therefore, organisations should have the flexibility to embed DPIAs into their corporate risk assessment processes and practices without having to resort to conducting a separate DPIA exercise mostly for documentation purposes under applicable data protection law.

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?

Neither agree nor disagree

There is merit in considering how self-assessment frameworks and risk mitigation can play a greater role in delivering better outcomes for controllers, people, and the regulator for smaller business or different sectors.

To make a success of this performing risk assessments in a robust, defensible, explainable and repeatable way will be vital for compliance, due diligence and for citizens to understand how their data is being handles and seek redress.

If the Government proposes to remove the need for a data protection impact assessment, guidance will be needed in its place to allow companies to confidently undertake risk assessments with guidance from the regulator should they choose to do so.

It is important that if the Government chooses to remove Data Protection Impact Assessments there is a clear statement that guidance from the regulator will be forthcoming.

Some members are concerned that the removal of DPIAs may be perceived by other regions as a reduction in protection of personal data which may be a risk to global data sharing agreements. It is therefore vital that any replacement self-assessment frameworks and risk mitigation seeks to achieve similar outcomes to DPIAs.

Prior consultation requirements

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

In the experience of our members, some organisations are reluctant to approach the ICO to discuss novel or high-risk processing and would instead implement mitigations to ensure compliance.

Members therefore welcome the proposal for the ICO to set out a list of processing activities that it considers to be high risk for clarity.

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

Yes, and the ICO should be encouraged to give legal comfort to companies to pursue this processing where the organisation can demonstrate that risks have been mitigated.

If no resolution can be found during a voluntary consultation process, it should be clear that this will not automatically trigger an investigation or have an adverse impact on any future investigation.

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

To help facilitate greater communication and collaboration between the ICO and industry, members suggest the following: (1) clarity on what the ICO considers high risk processing under Article 36; (2) confidence that any voluntary discussions on data processing would not lead to enforcement; (3) recognition of consultation with

the ICO as a mitigating action during any future investigation or enforcement action; (4) the ability to approach the ICO on an informal basis e.g. through a helpline

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?

Neither agree nor disagree

Although our members – particularly smaller organisations – find that this requirement can be burdensome, there are also many benefits in adhering to this requirement, and many larger organisations (particularly those operating in multiple jurisdictions) will continue to do so eg. For compliance purposes, record keeping and when working with external organisations, customers and TPPs, incident responses in the event of data breaches etc

Our members would welcome greater flexibility to take a more tailored approach to record keeping, proportionate to the volume and type of data processing being undertaken, or keeping requirements for certain circumstances eg. Business-critical services.

However, we would ask that where possible and in the guidance the UK seeks to find a way to recognise record keeping standards across multiple jurisdictions (e.g. UK, EU, etc).

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?

Somewhat agree

Increasing the threshold for notifying personal data breaches has the potential to reduce burdens on organisations – particularly for smaller organisations – in terms of cost and time. This will also have benefits for the resources of the ICO.

Organisations should be encouraged to develop and maintain a mature incident management program that can apply a risk-based assessment without having to notify the ICO of virtually every single incident on a 'better safe than sorry' basis. This ultimately provides very little value-add from an incident mitigation standpoint

However, if such changes are implemented, members would welcome the development of guidance and clear examples to support organisations in confidently interpreting and applying the new thresholds. This will also be important for citizens

to seek redress. Members would also welcome more ICO guidance on what constitutes a material and non-material risk to data subjects.

Members have also raised concern that any significant adjustment and increasing to the threshold may challenge both the UK's reputation as a high standard for data protection as well as consumer's rights to transparency. Therefore, any new guidance or breach reporting requirement must be informed by clear guidance not just for firms but also for citizens.

Finally, members urge the Government to also take into consideration the breach reporting requirements under PECR, where a lack of materiality threshold attached to this obligation means communications providers typically report far more breaches under PECR than under GDPR. Therefore, we recommend that any changes to reporting requirements designed to address concerns about over-reporting and administrative overhead are reflected equally across UK GDPR and PECR data breach reporting duties.

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

techUK strongly supports this approach as we believe this will help build a more collaborative relationship between the ICO and the companies it regulates with process and business innovation-based responses being prioritised over fines and regulatory action.

Ultimately this is beneficial for both the regulator, the business and the consumer by creating a more regular dialogue between the ICO and its constituents and more timely outcomes for data subjects as well as incentivising businesses to seek informal guidance from the ICO to seek updates to their data management practices.

Where an enforcement matter has wider implications, for example for competition because of the involvement of a firm with strategic market status, this process should include an impact assessment and consultation with competing firms. DRCF coordination should also be considered.

Further questions

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?

In the experience of our members, there is a general lack of awareness and understanding of data protection risks across organisations and more work can be done to upskill the UK's workforce. We recommend that Government considers what skills may be needed to implement PMPs, including clear examples of what good looks like.

Members have also suggested that encryption with non-repudiation be considered as a potential safeguard.

Record-keeping - 2

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?

techUK members have identified that records of processing activities (ROPA) can offer organisations benefits including: (1) acts as a quick point of reference in the event of investigating a potential data breach; (2) simplifies due diligence; (3) improves risk management of the supply chain and (4) acts as a single record of reference for lawful basis against a business process.

However, SMEs may welcome any changes that would reduce the burdens of compliance with Article 30.

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

Somewhat disagree

Changes to the reporting requirements may have undesirable knock-on effects for organisations' internal processes e.g, supplier arrangements. It would also add additional burden on organisations to develop new training and awareness raising initiatives for staff.

Further questions

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

techUK supports the privacy management programme and wishes to see it introduced. However, whether it is or isn't there is a broader point that needs to be

raised with Government on preventing duplication between the UK regime and other international approaches. This would apply to PMPs as well as the other proposed reforms to record keeping, breach reporting requirements and data protection officers.

It is vital that in all these cases that other similar approaches such as the existing privacy policies approach, existing breach notifications threshold and record keeping requirements are still permitted (without change) for companies operating in the UK. They should simply be recognised as compliant.

It is our understanding the Government intends to allow for this however this should be made clear in the Government's response to the consultation.

The clear benefit here is to reduce the burdens of compliance duplication for firms (UK headquartered or otherwise) who operate internationally and therefore for the purposes of running the business most efficiently may comply with different but similar standards, i.e. the existing standards currently in use in the UK which will remain applicable in the EU and other jurisdictions.

The advantage of allowing this to continue where they meet the UK's data protection principles is that it does not reduce the UK's attractiveness to operate as a global business, but also creates the space for a more tailored regime for businesses which start and scale in the UK before shifting to a more globally focused approach (as they would need to do in any case due to the extra territorial nature of various data protection regimes) when they reach later stages of their growth.

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.

In the experience of our members, SARs can be especially time consuming and costly. In some cases, members receive vexatious SARs, repeat and duplicate SARs, or some which are not made with the intention of understanding data processing e.g. solicitors and TPPs encouraging use of SARs to advance legal proceedings, or customers seeking information in the context of a complaint of grievance,

Although members recognise under the current rules, circumstances allow data controllers to refuse a SAR, or charge a fee for responding to it, it can be difficult for organisations to know in advance whether an SAR is genuine, making it difficult to operationalise such exceptions, especially when considering large organisations may handle thousands of SARs each year.

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

Somewhat agree

It would be helpful to clarify that the data subject has a duty to provide some context to its request if the request would otherwise require the company to use costly and/or time-sensitive resources and tools to search unstructured data repositories (e.g. unlimited email searches) with cannot be reasonably justified solely on the off chance that some of these repositories may contain incidental information about the data subject.

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?

Neither agree not disagree.

For the reasons mentioned above, we agree that introducing a cost limit and threshold for response could greatly help alleviate the administrative burden on companies, as well as reduce the cost to process DSARs.

However, there are risks in this approach. This will be likely be complex to implement and could create more obstructions to both organisations and consumers. For example, a cost limit would likely need to justifiable, and it is not clear what evidence is required to support this.

If implemented, clear guidance should be produced on this by the regulator and there should be avenues for consumers to challenge an organisations decision on this. Members have expressed a preference for organisations being given the ability to ask data subjects to narrow their request or provide further specificity on the information they seek in scenarios where they exceed the cost limit, rather than a default obligation to provide assistance.

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

techUK does not see a strong case for the reintroduction of a nominal fee. This could be viewed by citizens and other jurisdictions around the world as rolling back rights of individuals to make requests about how companies handle their data, while it would likely not serve as a deterrent for unreasonable requests

Members have not called for the reintroduction of the fee and requiring virtually all companies to establish systems to process such a fee would be onerous.

We also have concerns that a flat fee may also have particularly negative impacts on data subjects with low incomes.

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

Please see below some suggestions from our members:

- We believe subject access requests should be 'purposeful'. One measure that would help businesses to cope with the high amount of data access request (as well as delivering qualitative response) would be for data subject to identify the 'purpose' of their request and be required to specify the particular data processing activity. This way companies would be better positioned to concentrate their resource on locating and disclosing specific data rather than 'everything'. In addition, Government should consider steps it could take to deter vexatious requests in order to minimise this burden on UK businesses.

- Additional guidance on email searches and redaction exemptions (e.g. for business confidential information that only contains repetitive non-sensitive business information about the data subject) would be welcome, as well as further clarity as to what would meet the "manifestly unfounded" threshold. That is, the request would be "manifestly unfounded" unless it can be demonstrated that the organisation is not complying with data protection law in respect of the data subject or respecting the privacy of the data subject requesting access to their data.

- Our members believe that providing legal certainty on the "manifestly unfounded" threshold will ensure that customer trust We believe that providing legal certainty on the "manifestly unfounded" threshold will ensure that customer trust in the UK's data protection regime continues to be maintained, without creating 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'?

Based on feedback from our members, 'analytics' should exclude: (1) diagnostics-related processing which is used directly to ensure a service works properly, and (2) cookies which are directly used to enhance customer experience or engagement, but should include processing for audience measurement, general business analysis and wider product improvement.

Regulators, such as the CNIL in France, have taken a more flexible approach as to what constitutes an "essential" cookie.

These cookies could also be recategorised as “analytics” to enable personalised content and advertising to be served where a consumer has given their prior consent to processing for that purpose.

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

The analytics-related processing conducted by some of our members is carried out with the intention of drawing out a general understanding of performance or engagement of services, or for cybersecurity purposes, rather than with intention of exercising individual-level impacts. Therefore, analytics cookies are highly depended on by organisations to understand how their services are being used.

Under GDPR, these use cases fit under legitimate interests, but the consent requirement under PECR rules this out completely.

This has given rise to the proliferation of ‘cookie banners’, the curtailment of beneficial data uses by businesses with significant downside effects for the digital economy and innovation and, most importantly, without necessarily corresponding privacy benefits for people. Therefore, the collection of data by the cookie and the purpose of use of the data collected through it should be governed by the same legal basis that the organisation chooses to rely on under Article 6 UK GDPR.

Under the current rules, Cookies and other technologies are subject to the consent requirements before their use and placement. As per the above, their use and deployment should not be subject to PECR but instead the UK GDPR. Unifying the rules and creating clarity for businesses and users alike.

It is important to note that the UK GDPR makes clear that the collection and processing of all personal data must adhere to the obligations set down in UK GDPR for lawfulness, data minimisation, fairness, transparency and robust rights like objection, access, rectification, and deletion. In the absence of a requirement to adhere to the provisions of the ePrivacy Directive, we support initiatives by the Government to amend PECR accordingly. This clarification will also reduce consent fatigue among consumers for this low-risk type of processing.

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

Members would welcome removal of consent requirements set out in PECR and to align them to the criteria set out under GDPR. Many activities processed under legitimate interest are nullified once subject to requirements under PECR, where processing activity involves storage of or access to information on terminal equipment.

The Government should also continue to assess the EU e-Privacy legislation in this area and adopt elements of best practice to (1) avoid a double compliance burden for organisations operating website across borders and; (2) to ensure legal certainty for organisations, which is vital for innovation.

For further information see our answer to Q2.4.2.

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:

We agree with the proposal to remove the consent requirement for cookies (and other technologies). Controllers which wish to use such tools should be afforded the ability to rely on Article 6 UK GDPR, in the same manner as is the case for all other data collection and processing activities.

For further information see our answer to Q2.4.2.

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?

We are supportive of both the development of Codes of Conduct and regulatory guidance.

Regulatory guidance such as a certification mechanisms, seals and marks, would go towards providing clarity around the use of cookies. We believe this clarity would yield significant benefits for consumers, businesses (particularly small businesses), and the regulator.

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?

UK GDPR rules are built on the principle of individual accountability of each data controller with a data subject, including for obtaining consent.

A consent mechanism may provide people with a way to minimise this friction, potentially allowing them to signal a blanket preference for how they want data to be

collected and used by websites and services. However, allowing a third party to intermediate the relationship between controller and data subject may create compliance issues for data controllers and deny those companies, such as news providers, the ability to build trusted relationships directly with their customers.

Government must also consider this in the light of the CMA's conclusions about the structure of the browser market and the exercise of market power, as well as its investigation about the impact changes to how browsers and operating systems work could have on competition, for example in the digital advertising market.

With this in mind, it is critical that any proposed mechanism is developed in consultation with industry stakeholders, taking into account the evolving state of technology, different markets and cybersecurity best practices.

Government should also be mindful of the potential risks posed to vulnerable users and consider the additional education and awareness raising initiatives that should be implemented to ensure such services are inclusive.

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

See response to question 2.4.6 above.

Q2.4.10. What are the benefits and risks of updating the ICO's enforcement powers so that they can take action against organisations for the number of unsolicited direct marketing calls 'sent'?

This change is welcomed by techUK members.

Q2.4.11. What are the benefits and risks of introducing a 'duty to report' on communication service providers?

This duty would require communication service providers to inform the ICO when they have identified suspicious traffic transiting their networks. Currently the ICO has to rely on receiving complaints from users before they can request relevant information from communication service providers.

techUK members see little benefit in introducing a "duty to report" on communication providers, as this would simply add burden without tackling the root cause of problematic traffic. This is an area where Government, telecommunications providers, the ICO and law enforcement are generally aligned. Therefore, self-regulation and co-ordination through industry bodies is preferable to imposing additional obligations on operators.

In addition, there are already a number of industry specific efforts aimed at the reduction of the potential harm, as detailed below:

- Communication providers have regulatory obligations under Ofcom's General Conditions to identify and prevent calls with invalid calling line identification (CLI) data from reaching call recipients where technically feasible. Providers also must provide free calling line identification facilities to end-users so that they can also identify and make a conscious choice whether to respond or not to any suspicious call[5].

- Ofcom has a voluntary technical memorandum of understanding in place with a number of the larger communications providers and some transit providers to take additional prevention measures – the latest versions being less than 12 months old[6].

- Communication providers normally have commercial agreements around Artificially Inflated Traffic (AIT) which seeks to prevent those actors sending large amounts of call traffic which could be considered suspicious.

We would encourage the ICO to continue to instead work with Ofcom on this area, as there is a real risk of enforcing duplicative and inconsistent obligations on communications providers. If requirements are to be implemented, they should be proportionate, efficient and should not place any additional burden on organisations to report this information.

Q2.4.12. What, if any, other measures would help to reduce the number of unsolicited direct marketing calls and text messages and fraudulent calls and text messages?

Making it easier for companies and organisations to share data between themselves for the purposes of protection of customers would be one measure.

Q2.4.13. Do you see a case for legislative measures to combat nuisance calls and text messages?

No, our members consider that there are already sufficient powers held by Ofcom and the ICO to address this issue.

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

Based on member feedback, placing a legal mandate will not assist in reducing the number of nuisance and fraudulent calls.

---

[5] See Condition C6.6 and accompanying guidance: https://www.ofcom.org.uk/__data/assets/pdf_file/0021/112692/Consolidated-General-Conditions.pdf and https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/telecoms-industry-guidance/calling-line-identification

[6] https://www.ofcom.org.uk/__data/assets/pdf_file/0026/31859/nuisance_calls-tech-mou.pdf and https://www.ofcom.org.uk/__data/assets/pdf_file/0023/209093/nuisance-calls-tech-mou-transit.pdf

As noted above, there are already obligations in place on UK communications providers under Ofcom's General Conditions to identify and prevent calls with invalid calling line identification data (CLI) from reaching call recipients where technically feasible.

Members have also raised practical concerns about proposals to block calls and text messages "at source". These risks should be taken into consideration if any changes are considered:

- Challenges in identifying what is and is not legitimate traffic may lead to commercial or social communications being mistakenly blocked.
- Technical limitations which may cause legitimate calls from appearing "suspicious" eg. Traffic originating abroad.

Q2.4.15 What are the benefits and risks of providing free of charge services that block, where technically feasible, incoming calls from numbers not on an 'allow list'? An 'allow list' is a list of approved numbers that a phone will only accept incoming calls from.

Based on member feedback, the offering of this service is not recommended and is instead best tackled as a commercial matter.

The PECR already provides the necessary statutory instruments to enable the termination of automatic call forwarding, the prevention of calling line identification and the tracing of malicious or nuisance calls.

If this were to be implemented, we strongly call for the "technically feasible" caveat to remain in place (as it is for similar regulation from Ofcom).

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)?

Despite overlap between PECR and GDPR, Government should take into consideration the industries that are subject to both pieces of legislation (eg. Telecoms), and therefore have double/duplicative compliance responsibilities. Any changes made to penalties should ensure that particular industries are not disproportionately impacted as a result.

Rather than increasing PECR fines, our members see more benefit in adopting a voluntary undertakings process, wherein organisations provide a remedial action plan upon identifying an infringement which the ICO may authorise without taking any further action.

Q2.4.17. To what extent do you agree with allowing the ICO to impose assessment notices on organisations suspected of infringements of PECR to allow them to carry out audits of the organisation's processing activities?

Audits are costly so the threshold would need to be sufficiently high if government were minded to consider this.

Q2.4.18. Are there any other measures that would help to ensure that PECR's enforcement regime is effective, proportionate and dissuasive?

We note that the European Commission has been working on a revised E-Privacy Regulation for some time. However, there is a debate to be had around whether or not a separate piece of legislation is required. techUK would be keen for the UK to take a critical view of whether PECR is still required in light of the UK GDPR being in place.

Chapter 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?

Strongly agree

This is something techUK has long advocated for and we support the position outlined by the Government in its mission statement for approaching international data transfers in August 2021.

To ensure the UK's approach to future adequacy agreements is seen as high standard we would encourage the Government to continue with its current approach to transparency, for example in the way the Government published its explanatory framework for adequacy discussions with the EU and the publication of the recent manuals for adequacy assessments for third countries.

It is vitally important that the Government's approach to adequacy agreements takes account of the risk of onward transfers from jurisdictions which share an adequacy determination on to those that do not. This is vital for UK citizens data as well as the data of any partner countries the UK has an adequacy determination with. techUK therefore strongly supports strong guidance and assessment criteria in relation to onward transfers of any UK adequacy decisions.

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

techUK agrees with this approach and sees it as a practical step. However, it is vital that such a process is only completed for groups countries, regions and multilateral frameworks where the data protection framework is consistent in legislation and updated for the entire grouping through a common legislative process. For example, the EU and the EU GDPR.

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

This is a practical step which will reduce administrative burdens on the UK.

However, we would urge the Government to set out what changes to data protection systems or events would trigger an investigation or a review by the UK. I.e. legislative change or examples of issues/events relating outcomes on the ground that would

cause concern. This would also be useful for businesses as they review the medium- and long-term data export and import strategies.

Government should also create a reporting function so businesses and citizens can raise concerns where they believe data protection standards on the ground in a given jurisdiction are in decline.

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

Ensuring effective redress in third countries is vital to building consumer confidence into the UK's international transfer framework and businesses ability to use it. We therefore support this approach and would welcome guidance for consumers on how to exercise their rights in different jurisdictions.

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?

Somewhat agree

We agree with this approach in principle, however many businesses, particularly smaller ones will continue to use template standard contractual means to cover international data transfers. This will be due to a large number of smaller companies unable to perform risk assessments for day-to-day transfers.

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?

techUK supports the approach taken by the ICO in setting out the International Data Transfer Agreement and International Data Transfer Risk Assessment. The spirit of this approach should be continued in future to support clear and understandable risk assessments as well as standardised addendums to align contracts if they cannot be mutually recognised.

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

This is an eminently sensible reform which will significantly reduce the burden on businesses and would not undermine data protection standards.

However, guidance provided by the regulator should be clear under what transfer scenarios this exemption is operable and at what point the data being handled becomes subject to the UK transfer regime and the UK's data protection legislation. Clear guidance here will help businesses, particularly smaller businesses who stand most to benefit from this reform, to take full advantage of these proposals.

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 nor disagree

techUK cannot identify a strong demand from members for such a reform. Such a function would likely only be utilised by large companies able to effectively design and assess the risks and appropriateness of such a transfer mechanism. However, as many companies of this size will be required to design data transfer policies that can satisfy multiple jurisdictions in any case it's not clear how widely this reform would be used,

While that does not mean these proposals should not be taken forward, we see its benefits as limited.

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?

Guidance and templates should be provided to clarify what such alternative transfer mechanisms might be, and how to assess their appropriateness. Government should consider the different use cases in which templates may be required as a one-size-fits-all approach may lead to ambiguity for organisations. Additionally, advice and consultation should be offered to organisations for more complex transfers which involve a higher risk to personal data.

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?

Yes

This follows the approach taken by the ICO in International Data Transfer Agreement addendum. Any assessment of protections provided for in another country's legislation should be made by the ICO on the basis that they provide similar levels of protection to those operational under UK law.

This is consistent with a risk-based approach and would reduce unnecessary compliance burdens on companies. For example, we believe there is a strong case to recognise the level of protection offered under EU SCCs. This would also have business benefits given the existing reliance on these SCCs by a large number of organisations in the UK.

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 disagree

techUK does not see a compelling reason for the creation of a specific power. Recognition of new alternative transfer mechanisms via Secondary Legislation offers sufficient flexibility while also retaining Parliamentary oversight.

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?

Yes, certification schemes could be helpful in complex supply chains involving multiple parties that have to work together to ensure compliance with GDPR for end users.

3.5 Derogrations:

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

Allowing repetitive use of derogations is welcome as their use can be vital for companies and organisations caught short by a need to carry out atypical international transfers for a limited period of time. In line with previous comments guidance produced by the regulator should provide clarity and defensibility for the circumstances under which the repeat use of derogations can be used.

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.

Data is a global business, both UK headquartered and international companies operating in the UK regularly engage in data transfers with business partners across the globe. Securing access to data transfers is not just an issue for the tech sector, with the operations and supply chains of virtually every modern business supported by the transferring of personal data, whether that is detailed data sets for complex digital services, or the financial and logistical information needed for the trade in goods. To achieve the objectives of Mission 2 and secure 'pro-growth and trusted data regime' the UK needs to be seen as a trusted destination for data transfers.

While adequacy decisions such as the UK's adequacy decision from the EU helps reduce business burdens, its symbolic importance is arguably just as vital for allowing businesses and investors to make a strong case based on the perception of high standards of data protection in the UK.

Adequacy with the EU was a key ask of the sector during the EU exit transition. Through the proposed reforms in this consultation the UK can make the changes needed to boost growth and innovation. However, doing so while also maintaining access to global data flows, such as through EU adequacy, is the most effective way to succeed in achieving Mission 2 of the National Data Strategy. The UK needs to ensure that it strikes the right balance between reforms and not risking the loss of adequacy through the real or perceived lack of protection of personal data.

Chapter 4 - Delivering better public services

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

Somewhat disagree

It is not clear from the question whether it relates to the reporting of the fact that an algorithm is used for government decision-making or stipulates disclosure of the algorithm itself.

Being explicit about AI-powered solutions and top-level reporting of what data is being used, how, by whom and for what purpose can, indeed, improve public trust in government use of data.

Conversely, given inherent complexity of algorithms, providing technical details of algorithms is unlikely to build public trust as the public will not be able to assess their validity, safety and governance. Moreover, an overly aggressive transparency rule could chill development and/or jeopardize AI systems, e.g. if the transparency detail allows the systems to be manipulated or creates security/tampering risks.

It is also important to balance public interest in AI transparency on the one hand, with the intellectual property needs of research and business organisations on the other. Developers and owners of AI have a legitimate interest in protecting the intellectual property and confidential know-how that they develop.

Finally, any compliance burden should be proportionate to the aims of the legislation and not be such as to discourage further investment by companies into these areas.

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

Reasonable transparency requirements might include things like:

- Providing a general description of how the AI is intended to be used, the model's inputs and outputs, the types of data used to train the AI, and the basic factors that drive the algorithmic decisions. The goal in providing these descriptions should be that they are high-level, understandable by non-experts, and allow AI owners/developers to exclude confidential information and intellectual property. (It should be noted that specifications that require advanced training and expertise are not meaningful or useful to the general public for the rationale of enhancing trust. This will only enhance confusion over AI instead of explaining algorithmic decision-making.)

- Providing disclosure of an entity's voluntarily established code of conduct or principles on the responsible use of AI, or general information about the entity's AI governance process to inspire public trust and confidence.

- Providing a description of how an entity will help those affected by the AI decision-making understand their individual outcome and the AI reasoning (i.e., the process around how an entity will maintain public trust and confidence in response to individual AI outcomes).

- Providing a description of how bias is being assessed and remediated within the AI. Another possibility may be a requirement to confirm that AI testing has been conducted to determine if the algorithm equally treats specific protected groups.

From an IP perspective we would advocate against more aggressive reporting requirements for detailed technical specifications that include confidential information or intellectual property, or providing access to or copies of source code. As previously noted, this level of detail adversely impacts the IP rights of owners/developers, and can introduce security risks to the AI. It can also enhance confusion by general consumers if they cannot easily understand the disclosure. A confidential audit or protected review of AI (allowing trade secret materials to be protected to the greatest extent possible) may be a reasonable middle ground in specific circumstances where further AI review is required.

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

This proposal does not account for the unique sensitivities and complexities associated with health and health care delivery. If the implemented reporting includes data at a level of granularity that reveals a person's health or health care information it risks undermining public trust. The proposal may need to include a carve out for health data and health care data, or a clarification that only high-level summaries would be expected, rather than individual-level data in order to protect personal information.

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

We agree that it may be very hard to distinguish between the two. It will always of course depend on the context. Also, it is suggested that defining 'substantial' public interest is likely to be subjective and therefore could vary depending on whether you view the situation from an individual or group perspective, as well as given the situation in question could also shift and evolve overtime.

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

Somewhat agree:

Extensive stakeholder engagement with a diverse range of people will be required to consider and consult on any definition that is proposed. If this proposal was taken forward it will be important that there is a clear single point of contact for organisations seeking further clarification and guidance as and when it is needed.

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 disagree

This option is seen as unsustainable as it would require continual updating of the specific situations in scope. To accommodate all scenarios this list could risk becoming quite granular, making it difficult for companies to refer to and operationalise in practice.

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

Clarifying the rules in this area would be beneficial and welcomed particularly around the legislation that governs the retention of biometric data. For example, for custody images the rules of retention are currently not set out in legislation and therefore open to interpretation. Clarity and overall simplification could both increase police forces confidence in the rule that apply and public understanding and trust in this area.

4.5 Public Safety and National Security

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

Strongly agree

Government should ensure that the important role of the private sector in law enforcement and national security is reflected.

Chapter 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?

Strongly agree

A key strength for the UK is the experience, expertise, and global reputation of the ICO. It is seen around the globe as a respected, well resourced, independent, world leading data protection regulator. In the UK the ICO continues to play an important role for industry as a regulator that provides certainty on issues and areas that are increasingly complex and overlapping, supports compliance across both the public and private sector and has championed the importance of coordination and engagement between Regulators on data related issues.

This consultation provides an opportunity to consider how and where the ICO could be even more effective as a regulator that can support, guide, oversee and enable frictionless and meaningful compliance with data protection laws.

As the UK looks to create a national approach that is pragmatic, modern and pioneering the ICO will be key in providing expert advice and clear guidance to government, regulators, policy makers, industry and other key stakeholders on how data protection rules should be understood, interpreted and applied.

By providing regulatory certainty the ICO can support the UK's goal of being a leader of a modern, agile, flexible and innovative data protection system and regime that supports and encourages cutting edge innovation and builds meaningful data trust and confidence.

However, it is also important that the structure of the ICO, the way it works and practices that may need to be put in place continue to be seen as truly independent and able to support a systemic UK approach to data protection that is modern, agile, and innovative. This will mean a clear role for the ICO and the necessary resources it will need to be focused on providing government and industry with legal and regulatory clarity through the development of guidance, advice, enforcement and oversight.

Given the proposed increased scope and functions of the ICO the development of a clear "set of statutory strategic objectives for the ICO" is supported. This could help to provide clarity to industry and citizens as to where the remit and responsibility of the ICO starts and ends. It is important however that consideration and clarity is given to how often the statutory framework is reviewed and updated to ensure that the ICO's strategic objectives and duties remain relevant and appropriate to the wider UK data ecosystem and landscape.

The consultations clarification that the ICO would be left to set its operational objectives is welcomed. Also is the recognition of the ICO as an independent

regulator. However, as well as stating that the ICO is an independent regulator it is important that the ICO must also be seen to be acting independently against the strategic overall framework it has been given.

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?

Somewhat agree

The introduction of these two new elements to the ICO's objectives are understood and supported in principle. However, further details and understanding would be welcomed on what these new objectives would mean in practice and in reality. For example, further clarification would be welcomed on what the introduction of these two new obligations would result in terms of specific duties, activity or action that is envisaged to be taken forward by the ICO.

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

No

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?

Somewhat agree

Government has made it a strategic goal that regulation should enable innovation and growth in the digital economy. The proposed introduction of a duty to have regard to economic growth and innovation is supported.

However, when introducing this new duty it is suggested that the "specific obligations" could be enhanced by introducing a requirement for the ICO to engage regularly with innovators across all sectors of the economy to ensure the ICO develops, and keep up to date, an understanding and knowledge about how innovative business models work in practice and how innovative industries that are powered by data are developing.

This would ensure that the ICO is required to keep up to date with their understanding of industries and business models that are driving economic growth and innovation in the UK.

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

The proposal to introduce a duty for the ICO to have regard to competition is supported. Given the increasing role of data protection rules in the economic regulation of digital services, it is crucial that the ICO routinely assesses the impact on competition of the interpretation and enforcement options available. The recent recruitment of economists at the ICO to assess the economic impact of this decisions is a first step towards building this capability and is very welcome.

With respect to enforcement of competition rules, we believe that the CMA should remain the primary regulator and Government should not give the ICO concurrent powers. This would cause lack of clarity and confusion for businesses as to where to turn to on issue related to competition. The ICO and CMA already cooperate on shared issues through the DRCF and this should continue.

This cooperation would be helped by a clear process for the ICO to refer competition policy matters to the DRCF and an understanding that the ICO would, accordingly, defer decisions which could be detrimental to competition in digital markets.

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

As noted above, it is important that individual regulators do not exercise their powers in a way which conflicts with the objectives of other regulators or economic goals for the UK economy.

The establishment of the DCRF has been an important step forward in this regard and has been welcomed by our members. This is a great example of how the ICO, and therefore the UK, has shown global leadership in developing an establishing a pioneering way for regulators to work together, share understanding and help to identify common issues and challenges of regulating in a way that is predictable and coherent for digital businesses. This collaboration should and must continue, and a duty to cooperate would be a positive next step.

Q5.2.7. Are there any additional or alternative regulators to those in the Digital Regulation Cooperation Forum (CMA, Ofcom and FCA) that the duty on the ICO to cooperate and consult should apply to?

Don't know

Many digital markets have mature self-regulatory schemes so the DRCF regulators should, where relevant, seek to build relationships with such bodies and ensure that their regulatory decisions do not undermine successful self-regulation.

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?

Somewhat agree

While we agree with the objective to improve information sharing between regulators this is a proposal where further details and discussion is needed. If the proposed introduction of an information sharing gateway between the DRCF, and possibly wider with additional regulators, is to be taken forward it is important that clarity is built into this gateway as to what information would be shared, with whom, the exact purpose for when information would be shared and when the information sharing gateway can and should be used.

For example, what could be the specific purposes when information would be requested and on what basis would that information then be shared also how would it be decided if it was appropriate and proportionate for regulators to share information. Also, it should be clarified whether there would be any redress capability to challenge the sharing of information within the gateway.

These would be key safeguards that would need to be carefully thought through, developed and consulted on before any gateway is introduced.

In addition safeguards must be put in place to ensure information shared through the gateway remains protected and secured when in motion, at rest and throughout its lifecycle.

This includes how information will be deleted and removed when it is no longer needed for the purpose in which it was shared. Information shared with regulators can be commercially sensitive and confidential.

The entities supplying such information must be consulted on any sharing between the receiving regulator and other UK regulators, as well as any onward sharing with overseas regulators in order to preserve this confidentiality from inappropriately broad sharing or disclosure to competitors via legal discovery.

These reassurances are important to build confidence in, and engagement with, the DRCF by business.

Q5.2.9. Are there any additional or alternative regulators to those in the DRCF (ICO, CMA, Ofcom and FCA) that the information sharing gateway should include?

No

It is suggested that any information sharing gateway that is developed should be limited at the start to a small number of regulators before being rolled out to more. If this idea is to be taken forward starting with the current members of the DRCF, where there is existing structure of engagement and working practices, would be advised. We do not see a case for broader information sharing before further discussion, clarity and reassurances on the issues mentioned in 5.2.8 above are provided.

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?

Neither agree nor disagree

While such a periodic statement of strategic priorities (SPPs) would bring the ICO in line with other regulators such as Ofcom, we have some concerns around how such a statement would operate in practice.

We note that SPPs can be useful tools to formalise the Government's perspective on priorities without intruding on regulatory independence. However, for that to be the case, it is important that the Government carefully considers the parameters of the SPP.

A SPP could be particularly potentially problematic where it might have an impact on the ICOs regulatory remit to review the data protection practices and compliance of the Government and wider public sector. These might sensibly be kept out of scope, in the same way that the statement of strategic priorities for Ofcom does not cover sensitive issues within Ofcom's remit such as those relevant to freedom of expression.

The consultation makes it clear that the ICO would not be "bound" by the statement. This is an important and necessary condition of any ability to set up an SPP, and reflects the position with other regulators overseeing sensitive matters like Ofcom. However, it is not clear how the publication of this statement by the Secretary of State and a possible response from the ICO, as mentioned in the consultation document, would work in practice.

It is also unclear the regularity at which these statements might be produced. The consultation paper states they would be published "periodically". This is vauge and unhelpful. It is also not clear how open and transparent the proposed period of consultation, to be set by the Secretary of State, would be and who this would involve.

techUK would seek clarification on the concerns raised above. However, if the Government does progress with a periodic statement of strategic priorities this should be modelled on the approach taken by Ofcom, where such a statement is very infrequent and set at a high level.

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

The ICO's work on the international stage is important and a key asset to the UK. The UK's ability to be a global leader in the debate on the future of data governance,

particularly on the importance of global data flows is vital. It is important that the ICO's international work continues and is funded and resourced appropriately.

The publication of an international strategy would be welcomed. It is suggested however that this strategy is developed in consultation with key stakeholder including for instance government and Parliament. This could be away to ensure the strategy takes into consideration the Government's and UK's wider international policy priorities and objectives.

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?

Somewhat disagree

While it seems appropriate for the ICO's international work to be aligned with the objectives of the UK around the future of data governance on a global stage, it remains important that the ICO is seen, not just in the UK but around the world, as an independent regulator.

There is concern that a duty to require the ICO's international work to be aligned to the Government's international policy priorities could be seen by international partners as a reduction in the independence of the ICO. This could have serious implications for the ICO to lead and take part in discussions on issues including the future of adequacy and global data flows.

Instead, it is suggested that the ICO is required to consult on the development of its international strategy and involve Government and Parliament in this process to ensure its strategy is aligned to the wider international debate and objectives of the UK.

5.3 Governance Model and Leadership

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

Somewhat agree

The proposed introduction of an independent board and chief executive officer role at the ICO is supported as this brings the ICO into line with other existing regulators such as the FCA and Ofcom. However, the retention of the Information Commissioners title, for the chair of the new Board, is important and welcomed and strongly supported.

We agree that it is appropriate for the ICO's leadership and governance model to be aligned with that of other regulators. This will help ensure consistency of decisions, overall coherence and avoid authority being invested only in one individual.

Q5.3.2. To what extent do you agree with the use of the Public Appointment process for the new chair of the ICO?

Strongly agree

We believe this is the most appropriate process for the appointment of a chair of the ICO.

Q.5.3.3. To what extent do you agree with the use of the Public Appointment process for the non-executive members of the ICO's board?

Strongly agree

We believe this is the most appropriate process for the appointment of the non-executive members of the ICO's board.

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

Somewhat disagree

There is some concern as to the way in which the ICO's CEO would be appointed. As highlighted in the ICO's own response to the consultation, it would be more appropriate for the Board members to be appointed under the Public Appointment Process and then the Board to appoint the CEO.

This is the approach that is taken by other regulators including the Ofcom Board. This would allow the Board to replace the CEO if a situation were to occur where this was required. This approach would mean the ICO would be aligned with other UK regulators, which is a key theme running throughout Chapter 5 of the consultation. This consistency with the approach taken for regulators will be particularly important to the perceptions of the ICO's independence and given the ICO's role in regulating the public sector.

Q5.3.5. To what extent do you agree that the salary for the Information Commissioner (i.e. the proposed chair of the ICO in the future governance model) should not require Parliamentary approval?

Strongly agree

We do not believe the salary for the chair of the ICO should require Parliamentary approval.

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?

Strongly agree

We agree that the ICO should be publicly accountable for delivering on its duties. An affirmative obligation to report on how it has fulfilled these duties and the consequences of its regulatory decisions would be an important complement to the modernised governance structure proposed above.

Q5.4.2. To what extent do you agree with the proposal to introduce a requirement for the ICO to develop and publish comprehensive and meaningful key performance indicators (KPIs) to underpin its annual report?

Somewhat agree

While the proposals in this area are supported it should be recognised that the ICO has been an example of best practice in terms of its willingness and openness to engage and consult with stakeholders and the public on its activities and key work areas.

However, KPI's would be a helpful mechanism to help the ICO to report on how it has fulfilled its duties and the consequences of its regulatory decisions. However, implementation of KPI's should not lead to increased information requests to organisations as there is risk that the associated reporting obligations placed, will outweigh the benefit of the insights drawn from KPI tracking.

Q5.4.3. To what extent do you agree with the proposal to require the ICO to publish the key strategies and processes that guide its work?

Strongly agree

As above, this transparency would helpfully frame how it has fulfilled these duties and the consequences of its regulatory decisions and be useful transparency to stakeholders.

Q5.4.4. What, if any, further legislative or other measures with respect to reporting by the ICO would aid transparency and scrutiny of its performance?

No

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

As highlighted below to Q5.5.2 what would be useful as part of the ICO's consultation process is a requirement for the ICO to publish a response to the consultation input received during a formal consultation process. This is a requirement that currently exists for Government following the completion of a consultation process. This would be useful and helpful to show how the input received by the ICO during the consultation has been taken on board and, if the input has not been taken onboard, an explanation as to why this was not the case.

The ICO should also consult on its economic impact assessments and publish the assessments in advance of publishing any final decision.

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

Further, given a key duty of the ICO is to develop and produce guidance and opinions it is also suggested that consideration be given to providing information on how to raise and discuss the contents of guidance and/or opinions if and where concerns with the published guidance or opinions have been identified.

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

Neither agree nor disagree

While the idea of introducing an independent review of the ICO is interesting, it is questioned whether giving this power to DCMS would result in an independent review.

For example, to what extent is Government a third party? Particularly given the role of Government, and Parliament, in appointing key roles such as the ICO and the new suggested Chair of the Board, as well as the ICO's role in reviewing the government's compliance with data protection laws.

It is suggested that any review powers should be given to a truly third party. Also, further details should be developed, and consulted on, as to the specific "thresholds" that would have to be met for a review to be called.

Q5.4.7. Please share your views on what, if any, criteria ought to be used to establish a threshold for the ICO's performance below which the government may initiate an independent review.

We refer you to the answer to question 5.4.6 above.

5.5 Codes of Practice and Guidance

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

Somewhat agree

The development and publication of impact assessments would be welcomed. ICO guidance can apply to complex business models and supply chains and can impact multiple parties involved in the supply of a digital product or service. It is therefore essential that the ICO publish its assessment of potential impacts on all parties, including economic and competition impacts.

However, it would be useful to clarify at what stage in the process of consultation the impact assessment, which should include an assessment of the possible administrative burdens that codes of practice might introduce, should be developed and published. For example, at the start of a consultation on proposals or at the end assessment of the finalised Code of practice of guidance before the final version is published.

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?

Somewhat agree

While the proposal to have expert guidance is welcomed, the proposed requirement for the ICO to establish panels of persons to consult on the development of Code of Practice and guidance is one that requires further consideration. It will be important that expertise is sufficiently current, independent and impartial. There is a risk that this could add a step to the consultation process which could lead to delays in the development and then introduction of codes and guidance which is key to industry being able to move forward with data driven innovative ideas, products and services to the market or resolving issues affecting individuals' data rights.

Given the ICO's record of engagement and consultation on the development of Codes of Practice and guidance it is unclear what the creation of panels of experts would provide the ICO that is not able to be provided via the normal consultation process that exists today.

However, what would be useful as part of the ICO's consultation process is a requirement for the ICO to publish a response to the consultation input received during a formal consultation process. This is a requirement that currently exists for Government. This would be useful and helpful to show how the input received by the ICO during the consultation has been taken on board and, if the input has not been taken onboard, an explanation as to why this was not the case.

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

Given that the ICO's codes of practice and/or guidance could relate to the processing of data by Government departments and the public sector more broadly, it does not seem appropriate for the Secretary of State to have the powers to approve, or not approve, code of practice and guidance.

The introduction of this proposal would be seen to significantly undermine the independence of the ICO and therefore should not be taken forward.

Q5.5.4. The proposals under this section would apply to the ICO's codes of practice, and complex or novel guidance only. To what extent do you think these proposals should apply to a broader set of the ICO's regulatory products?

Neither agree nor disagree

Additional detail on this suggestion would be welcome, however any reform must seek to uphold the independence of the regulator.

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

Yes

Through this consultation the Government aims to put a greater emphasis on guidance from the regulator and to in this section introduce a duty to consider the economic and competition effects when producing new guidance. It therefore logically follows that the ICO should undertake and publish impact assessments on new guidance.

Impact assessments should be conducted for the majority of guidance issued with impact assessments only not issued where there is a strong case for new guidance to be issued quickly or where only minor tweaks are being made. In these cases the ICO should set out an analysis for why no impact assessment has been taken and endeavour where possible to set out an impact assessment after the guidance has been handed down and creating an opportunity for feedback.

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?

Somewhat agree

Given the significant resources the ICO currently uses to manage data-protection complaints, the development of a more “efficient and effective model” based on a “risk-based approach” seems appropriate.

However, there are some concerns with the suggested shift of full responsibly, and resource burden, of complaints to organisations, and the impact that this could have on SMEs.

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?

Somewhat agree

Given the right of redress being a fundamental principle of the UK Data Protection Act it is important that there is clarity and certainty for individuals and organisations in this important area.

The principle of accountability is foundational to UK data protection law and it is right that data controllers have an opportunity to resolve a data subject’s complaint before the ICO intervenes. In fact it is common practice right now for complainants to raise complaints directly with the relevant data controller and is the current ICO practice (“How we deal with compliants and concerns: A guide for data controllers”).

This approach makes complaint handling more efficient and avoids draining ICO’s resources on complaints that are easier to resolve. As a result this proposal could help to provide clarity by formalizing current practices on complaint handling and could play a key role in ensuring the ICO manages its resources effectively by only engaging in complaints once the individual has first attempted to resolve a compliant with the relevant data controller.

However, it is also vital that before any proposals in this area are taken forward that an assessment on the impact of businesses, of all size and sector, is undertaken to understand any economic and operational impacts the change might have on organisations, particularly SMEs.

Further details would also be needed as to when and how complaint would be able to be escalated to the ICO and who would be required to do this. For example, would individual data subjects be able to escalate complaints to the ICO or would the requirement be on the organisation that have received a complaint to raise this with the ICO.

Also further clarity would also be welcomed on how the ICO will be expected to investigate complaints lodged with the ICO and provide timely responses to consumers. If implemented, Government should also ensure that the ICO has full visibility of complaints in order to understand and have oversight of trends and themes.

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 agree

The proposal to require organisations to have a complaint handling process in place is another area where an impact assessment should be required before moving forward.

In particular to assess the impact such a requirement on SME and smaller organisations, such as charities. An assessment on the operational and economic impact of requiring data controllers to put in place a complaints-handling process, beyond what is already in place, is needed.

Many larger organisations will already have complaints handling processes in place. Therefore, if this proposal is implemented, Government should not include overly prescriptive guidance on what the complaint process should look like. This will offer organisations – all of which differ in circumstances – the ability to design a complaints process that is best suited to their business model.

Gudiance should be provide by the ICO to inform this process as well as provding guidance for companies to effectively deal with vexatious or repeat complaints.

Finally, the proposed requirement to publish the complaints handling procedure may simply increase organisations' regulatory burden without identifying a problem which needs to be remedied. Before implementing such a reform, Government should provide further clarity on the proposed challenge this change is aiming to resolve.

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

Ensuring that the ICO can use its discretion to focus on complaints that have significant impact is supported.

However, it is not clear why this needs to be introduced into legislation. It is suggested that the flexibility that the ICO currently has in this area should be maintained to ensure it can act as and when it deems most appropriate.

If the ICO seeks to pursue a complaint on the above grounds it should also be able to reach voluntary undertakings with data controllers to increase its the flexibility and seed in seeking to address complaints.

techUK would also welcome further clarification on what a “risk-based approach” to complaints would mean in practice.

5.7 Enforcement Powers

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?

Neither agree nor disagree

If the development of technical reports are to help support and inform the ICO’s investigation into a specific incident, the introduction of any new power should be clear in what would trigger the requirement for a technical report to be commissioned. For example, would there be a threshold of seriousness or risk to individuals’ data rights from an incident that would trigger the requirement for a technical report to be commissioned, and act as an appropriate safeguard to limit potential overuse by the ICO.

Also, it is important that in situations where the resolution of an investigation is timely, that the commissioning and conduction of an independent technical report does not lead to delays in the ICO’s formal investigations which could put at risk individuals’ data rights and organisations’ ability to operate. It is therefore suggested that consideration be given to introducing time limits for the development and production of technical reports in any new power that is developed. In addition, the ICO should consult with interested parties on technical reports. Such reports would need to keep commercially sensitive information confidential.

techUK would also welcome further clarity on who will have access to the findings of any independent technical report once published. Organisations should have the ability to respond to and review the report before enforcement.

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?

As the technical reports are to aid the ICO’s own investigations the cost of the reports should be borne by the ICO.

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

Organisations should not be required to pay for these technical reports which are to aid the ICO’s own investigations.

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?

Neither agree nor disagree

As the power to compel witnesses is an intrusive one, it should only be used in exceptional circumstances (e.g. where there has been a clear and serious violation of GDPR which is likely to cause severe damage or distress and is the result of deliberate breach or negligence).

Other regulators in the DCRF have such powers eg. Ofcom and CMA. Therefore, if implemented, Government should review this power in relation to other regulators and implement safeguards as necessary to inhibit misuse by the ICO. When exercising such a power, the ICO should take into consideration where compelled evidence may be inadmissible (e.g. in criminal proceedings, or in cross-border investigations where other authorities may accept compelled evidence).

Finally, this power should not be absolute, and individuals should not have to comply where they may have a "reasonable excuse" (e.g. if the evidence may put them in breach of law in another jurisdiction, or if they are being questioned on information subject to legal professional privilege.)

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?

Neither agree nor disagree

Please see the answer above to Q5.7.5.

Q5.7.7. To what extent do you agree with the proposal to amend the statutory deadline for the ICO to issue a penalty following a Notice of Intent in order to remove unnecessary deadlines on the investigations process?

Strongly disagree

techUK recommends that the statutory deadline between Notice of Intent and penalty should remain unchanged. It is not clear whether an extension would be an adequate solution and may simply lead to further delays in investigation processes. Delays often cause uncertainty to organisations, and can also be costly.

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

This should be considered a basic courtesy, to allow businesses to plan and resource their engagement with the ICO on all matters.

5.8 Biometrics Commissioner and Surveillance Camera Commissioner

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

There is a need for greater clarity and certainty of how the existing oversight and legal framework applies. For example, currently the guidance in this space is fragmented across different departments and bodies. This includes the, Surveillance Camera Code of Practices, Surveillance Camera Commissioner's best practice guidance for all police forces in England and Wales, Information Commissioner's Opinion piece on the use of live facial recognition technology by law enforcement in public places and wider Data Protection Act requirements and provisions under biometrics and human rights act.

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?

Somewhat agree

Bringing the functions of the Biometrics Commissioner and Surveillance Camera Commissioner's role into the ICO would be an important step in helping to provide greater alignment, clarity and certainty particularly where rulings are delivered by the existing regulators today. As the deployment of facial recognition technology is highly sensitive, clarity is important to give system operators confidence that all applicable legislation is being considered.

This move would also be a first around the world demonstrating how the UK is showing global leadership in understanding and addressing issues and concerns related to emerging technologies in this area, and creating a one-stop shop where industry and citizens can ask advice and guidance, to ensure data governance issues can be addressed appropriately.

However, if this proposal is to be taken forward it is vital that the functions of the Biometrics Commissioner and the Surveillance Camera Commissioner are given dedicated and sufficient resources and expertise within the ICO.