2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Which? Response to Data: A new direction consultation

19th November 2021

INTRODUCTION

Which? welcomes the opportunity to respond to the government's proposals for change to the UK's data protection regime, and to contribute the view of consumers on some of the critical areas that will impact them if changes to the UK's data protection and privacy laws are made.

Overall Which? continues to fully support the basic principles of the UK GDPR. However, we acknowledge that there is room for improvement to any regulation which needs to grow and adapt with societal and technological changes. Our view is that the UK GDPR provides a solid foundation on which to build. This is an opportunity to strengthen the existing regulation, develop it further, for example by enacting Article 80(2) and more broadly ensure greater clarity for business and data subjects alike.

Innovation and growth in the digital age relies on data. Consumers' data is at the heart of many commercial business models. It is vital therefore that consumers (as data subjects) are put front and centre of any data protection regime. It is also vital that future adaptation of a regime sets out to actively create a trusted environment in which the rights and protections for both data subjects and business are equal.

Which? welcomes the concept of a data protection regime being 'adaptable and dynamic', however we are concerned that the proposals in this strategy are so light touch and err so strongly towards deregulation that consumers will face reduced protection, a lack of control, a lack of clarity, and a lack of transparency about how personal and sensitive data is being used.

Similarly, our concern for business and organisations if the light touch approach were to be enforced, is that they will find defining their own more 'flexible' approach more burdensome and unclear than the current, more tightly defined requirements of the existing UK GDPR. Business and consumers alike want a clear and consistent framework: consumers want a clear understanding of their rights and to know what businesses are doing, and businesses want to know they are doing the right thing without ambiguity.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

We are well aware that there has been limited enforcement activity undertaken by the ICO since the regulation came into force. These proposals set out a more 'permissive' approach as do other recent government proposals, including the consultation on the Better Regulation Framework and the broader National Data Strategy. We are sceptical that moving to a more permissive approach is in the best interests of consumers.

It would be extremely disruptive for consumers and businesses if the UK's adequacy status were called into question. The adequacy decision is not only strictly limited by a 'sunset' clause that automatically expires in less than four years, but the EU Commission has said that the decision is subject to 'continual monitoring' and could be revoked at any time. We are concerned therefore about the impact of the proposed substantial legal changes on the UK being able to continue to rely on the current EU Adequacy Decision[1].

Our response to this consultation is focused on representing the best interests and rights of consumers as data subjects. We have used direct engagement with consumers to inform our response, and direct experience from Which? as a business implementing UK GDPR. Finally, we wish to emphasise that we have responded only to the questions that currently appear most relevant to consumers in relation to the specific proposals and where we have enough information to provide a robust response. As things develop we will look at suggested proposals as a whole and respond accordingly.

RESPONSE

CHAPTER 1 - REDUCING BARRIERS TO RESPONSIBLE INNOVATION

- **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?

While Which? agrees that research activities are very important, it should not be possible to gain unlimited consent to data on the basis that data may be useful at some point in the future, without being clear on the future uses and timeframes for data retention.

We do not agree that a new lawful ground for research should be added to Article 6 UK GDPR or otherwise included in the reform. It is important to maintain public trust in the use of data for research, as shown by the widespread concern about sharing of NHS data on individual patients without their informed consent, as recently demonstrated by patients in England in relation to the General Practice Data for Planning and Research (GPDPR) scheme.

[1] We also fully support Article 202(1) of the UK/EU Trade and Cooperation Agreement which provides, 'Each Party recognises that individuals have a right to the protection of personal data and privacy and that high standards in this regard contribute to trust in the digital economy and to the development of trade'.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Consumers are also likely to want to know whether, and to what extent, the data they provide for research purposes may also be used for commercial purposes. The starting point for using data in a research environment should be that clear justification must be provided for not anonymising personal data. In the meantime, we note that the ICO is developing updated guidance for researchers and we suggest that priority is given to this work instead of seeking to amend the UK GDPR.

- **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?
- **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**?**
- **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?

Which? agrees that the use of personal data can provide an important role in a range of scientific, medical and societal decisions and innovations. Which? does not agree that data subjects should be asked to consent to broader areas of scientific research that cannot be fully identified at the initial point of collection.

Which? believes that these unidentified purposes may exceed data subjects' expectations about what the data they provide will be used for. Furthermore the term 'scientific research' is broad and unclear and could mean a wide range of purposes including ones which may be considered unethical to some people's moral or religious beliefs, or refer to research undertaken by organisations that some may not wish to engage with.

The right for a person to know what, why, when, how and by whom data - particularly sensitive, special category or behavioural data such as lifestyle or wellbeing data - will be used is critical to developing and maintaining trust and transparency. Which? believes that data subjects should be informed of any further purpose and asked clearly to give new consent.

Consumer engagement research[2] undertaken by Which? in 2021 found that 72% of consumers are comfortable sharing health data from health apps with medical professionals such as their GP but only 31% of consumers would share this same data with a private company developing health or medical products and services.

[2] Which? Consumer Insight - Consumer attitudes to sharing their health app data, 2021.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Which? has already found that consumer trust is low when the information provided about how medical and health data will be used is lacking in detail. Of the people surveyed by Which? about awareness of the GPDPR scheme, 40% said they wanted to opt out.[3] As of Summer 2021, according to official figures 3.1 million people had chosen to opt out[4]. Our survey revealed that the reasons behind opting out included a lack of trust in who the data would be shared with, and worries about data being shared with, or sold to, US pharmaceutical companies. It is unclear whether this concern was founded, as the information provided about the scheme regarding who may have access to the data included broad-brush definitions of 'researchers'.

People want clarity as to what institutions or businesses researchers work for and for what scientific research the data is to be used. While it may not always be known who might use data in the future, ongoing communication with data subjects should not be viewed as inhibitive or restrictive for data use.

Requiring people to consent to future uses of data, potentially in perpetuity, may seem like a reasonable way of tackling this problem, but as the approach taken to the GPDPR clearly demonstrated, poor communication and reliance on 'opt out' rather than 'opt in', is seen by many as keeping people from the ability to make decisions about how data about them will be used and by whom. Not communicating clearly and honestly brings the risk that misinformation and disinformation will be spread regarding a project, leading to wider mistrust and fewer people consenting to data use for any purpose. This approach therefore represents a greater risk to society than an open approach that seeks to inform data subjects.

Furthermore, Which? believes that consent should take into consideration not just further use, but any and all aspects of use including (but not limited to) data management, handling, storage, anonymisation, and pseudonymisation.

The approach outlined from OpenSAFELY[5], whereby privacy and security controls are central to how researchers can access held data, is positive. The process of explaining how data will be managed, stored, and accessed at the point of collection is welcome. OpenSAFELY and Genomics England offer good examples of this approach in action.

More broadly, we oppose any moves to remove requirements for controllers to provide further information to data subjects before any further processing is undertaken, including for research purposes. We understand that in the recent emergency crisis of the Covid-19 pandemic special measures were put in place in order to deal with the crisis. We do not

[3] Which? News - NHS health data sharing: what you need to know about your medical data and GPDPR, July 2021
[4] NHS Digital, National Data Opt-Out
[5] University of Oxford About OpenSAFELY

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

believe that an emergency approach should be embedded in day-to-day practice. Article 13 UK GDPR should therefore be retained.

- **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?
- **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?
- **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**?**
- **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?

Which? believes that there is benefit in providing clarity on when further processing is lawful, including the compatibility test. Transparency is paramount here, so that data subjects can have confidence in how organisations are using their data, and businesses can have certainty that their activities are lawful. In particular, where the original lawful basis for processing was consent, there is a need to be transparent with individuals about any further processing, and for the individuals to retain control over how their data is re-used.

Which? does not believe that the exceptions to this rule should be extended beyond those already set out in UK GDPR and the Recitals.

A guidance document including examples, rather than significant changes to the legislative text, could be the best way of providing clarification here.

- **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?
- **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?

Which? is concerned by the proposal to create a limited exhaustive list of legitimate interests. A government-defined list used as a tick box exercise would miss the much needed context of the business in question, the nuance of the purpose and use of the data being collected. Any such list would not be guaranteed to provide the required depth of detail and scrutiny around consideration of data ethics, reasons for use, consideration of harms to data subjects or the necessity and proportionality of the data collection, retention and use. We do not believe that there is a one-size-fits-all solution here, nor that a 'suitably

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

generic' list would offer the right level of scrutiny as outlined, or be agile enough to respond to societal/technological change.

Recital 47 UK GDPR makes clear 'reasonable expectation' of the data subject is necessary. Some of the examples provided in the strategy document seem dubious and would not accord with people's 'reasonable expectations' - for example, 'business innovation to improve services' or delivering of 'public communications by non-public bodies'.

While there may be pushback from businesses on the need to interrogate fully why they want to collect, retain, share and use data, data subjects are a critical part of the data ecosystem - particularly consumer data collected in relation to products and services. Data subjects must therefore be considered or, wherever possible, given the choice to consent to the collection, retention and use of data about them.

Lowering the standard by deregulating to enable organisations to use 'legitimate interest' effectively as a coverall approach would undermine data subjects' rights. Recent enforcement action[6] by the Information Commissioner against credit reference agencies for lack of compliance with UK GDPR on data sharing with third parties provides a good illustration of the dangers of a less strict approach on the 'legitimate interests' grounds.

With regard to the list of legitimate interests, we address our thoughts on 61(d) in detail on pages 24 and 25 of this document.

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

Which? is unconvinced by the arguments and evidence made in the strategy document in relation to the problems with Article 6(1)(f).

The suggestion that there is an 'over-reliance' on consent is not substantiated. While we are aware of the arguments presented in the Taskforce on Innovation, Growth and Regulatory Reform (TIGRR) report, where the voice of business was presented, we are concerned that reference to 'some' controllers in the business sector finding UK GDPR complicated may be elevating the voices of a minority not the majority. Clarity on how many businesses are finding the law 'complicated' as opposed to awkward, would help shine light on exactly how big a problem this is and therefore how necessary such profound changes to UK data protection law actually are.

UK GDPR is still in its relative infancy, but overall the framework has provided a good starting point. Requiring businesses to adopt a brand new set of regulations so soon after they invested heavily in adopting the GDPR initially is an unnecessary disruption at a time when the business sector is already facing existing disruption from a range of enormous

[6] ICO, ICO takes enforcement action against Experian after data broking investigation, October 2020

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

factors; not least Covid-19 and new regulations following our withdrawal from the European Union. Which? therefore believes that UK GDPR is a framework to be built upon not dismantled. Strengthening data protection law will enable greater growth and innovation and clarity for people and businesses alike.

Weakening protections or resorting to tick-box coverall approaches - such as overarching legitimate interest without the need for a balancing test and deeper ethical consideration around the collection, retention and use of data - undermines all aspects of the data ecosystem.

While Which? supports strengthening the existing framework, this is not a case of additional safeguards being put in place. Rather we want to see the retention of a balancing test and clear transparency requirements in order to determine where legitimate interest is appropriate.

- **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?

Which? encourages ethical innovation and agrees there should be a safe regulatory space for the responsible development, testing and training of AI. However, Which? is concerned about the term 'use personal data more freely' and the lack of detail provided in the strategy about what that means. Furthermore, there is little detail provided about what the 'appropriate safeguards' will be and how they will actively ensure a data subject's privacy and security is not undermined.

The broad-brush term 'personal data' also needs to be given greater clarity and more granular explanation: what personal data, for what purpose, collected by whom, shared with and used by whom? Personal data covers such a broad spectrum, including identifying data, sensitive/special category data, behavioural data, profiling data, etc. It is vital that clarity, nuance and specificity is provided.

Finally, it must be stressed that freer use of, or access to, 'personal data' doesn't necessarily lead to good data quality or valuable or meaningful operational capability. Access to data is merely the first step in a much bigger journey of good data handling, labelling, cleaning, standards, etc. Much more detail is needed to explain how data will be handled to ensure testing and training is best facilitated.

- **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?

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

- **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?
- **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?

Which? is concerned by any reduction in protections around the consent, collection, use and storage of sensitive and special category data highlighted in questions 1.5.10 to 1.5.12. We are concerned that if the processing of personal data for the purposes outlined in question 1.5.10 are not subject to a balancing test, sensitive/special category personal data will be collected, stored and used for purposes that could exceed the data subject's consent given at the initial point of collection.

Checks and balances are needed in relation to sensitive personal data. We agree with the points in paragraph 92 of the strategy that raise concern that should paragraph 91b be adopted the result may be 'a disproportionate increase of processing of personal data of individuals with protected characteristics' and that 'the more an individual's personal data is processed, the greater the likelihood of intrusion into their private and family life, and the greater the risk of a breach involving their personal data' there may.

We appreciate the point that the proposal is to 'support organisations to monitor bias and eliminate discrimination'. However, we do not agree that legitimate interest for greater collection of identifiable sensitive data is necessarily the only solution to this. We are aware that anonymous collection of protected characteristic data is already regularly undertaken, including by government, thereby demonstrating that collection of sensitive data can be done without extending intrusion into a data user's family or personal life.

Sensitive personal data or data that is defined as 'protected characteristic' data must be protected. The depth to which it can be used to not just identify an individual but how it can be used to identify and discriminate against groups of people is profound. The suggestion that the more data that is collected, the more people will be protected is of serious concern. History has repeatedly shown that not to be the case. Indeed, the collection of data being used to easily identify groups has led to, and continues to lead to, serious harms, discrimination and genocide. As technologies become more advanced, regulation around the collection of sensitive data, such as biometric data, must be strengthened not weakened.

Bias and biased decisions do not come from lack of data; bias can be inbuilt accidentally or on purpose and can have little to do with the volume of data or the completeness of the data set. For example, bias can come from inaccurate data or it can come from someone making a decision based on an attempt to reduce bias. Just because a data set may be seen to be complete does not mean it is accurate or protected from subjectivity. Data collected by

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

consumer health wearables and apps, for example, are subject to inaccuracy and discrepancy. Bias that might arise from this data therefore would not be resolved by greater collection and use of the data, if the same inaccuracies persisted.

Which? opposes the weakening of protections or any deregulation in this area as we believe people's rights and freedoms must be protected, not undermined. We are opposed to the proposal to allow the processing of personal data for the purposes of ensuring AI systems' bias monitoring, detection and correction as a legitimate interest under Article 6(1)(f) for which the balancing test is not required. However, as long as the 'substantial public interest' approach is maintained, the processing of special category data is genuinely the only meaningful option to counteract AI bias and a full policy document in each case is still mandatory. The inclusion of a specific condition on this issue in Schedule 1 to the Data Protection Act 2018 may be helpful and provide further opportunities for transparency. We also urge the government and the ICO to work closely on this issue with the Equality and Human Rights Commission and other organisations in the equalities field representing those from groups that are disadvantaged and discriminated against.

Introduction to the questions relating to automated decision making and Article 22:

The proposals in the strategy document in relation to Article 22 and the detail provided make clear that this is a complex and still relatively nascent area.

With that in mind, Which? undertook a 6 day Community Engagement[7] with 22 consumers to learn what they understand in this area, their views of the benefits and risks and what their expectations are in relation to their rights in the future. We believe that hearing directly from consumers is vital to the debate and the development of regulation. Furthermore, it provides a necessary counterpoint to the views of business. We are presenting an overview of these findings here as an introduction to the questions related to Article 22 rather than a direct response. We have taken the views of the consumers into consideration in the answers we provide and our policy positions relating to Article 22.

When AI is used in consumer products and services to 'suggest' something to aid decision making - for example content on Netflix - the use of AI is considered by some to be helpful and efficient. But when AI is used to make a 'decision' about an individual, especially if the outcome of the decision could impact the consumer more seriously (e.g. in relation to insurance) then consumers felt it was necessary to have the right for a human to review the decision. They also felt decision making processes should be transparent. At present, AI is not yet viewed as fair or trustworthy. Additionally, there was concern about data getting into the wrong hands and about poor protection of privacy. One participant wrote that 'AI can be used to get you a better deal or to exploit you, and you can't tell which is which and what's being decided about you.'

[7] Which? The Consumer Voice: Automated Decision Making and Cookie Consents proposed by Data: A new direction; Which? November 2021

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

There was a strong belief that the right to challenge should exist and that human intervention should always be an option. Consumers felt the removal of the right to challenge was of no benefit to consumers and would be unfair. One consumer felt the right to challenge was 'a right not a privilege'. Some participants felt removal of the right would be 'dehumanising', and 'gives too much power to fallible systems that could have unintended consequences'. Concerns were raised about AI missing the 'context' of situations - this was raised as a concern particularly in relation to AI used in 'huge decisions about my life', where nuance is needed. This was emphasised by others who said the 'best questions in real life are not black and white, yes versus no'. It was viewed that automated decisions tend to be binary, 'devoid of social context, compassion, moral and social ethics and curiosity', which made people feel uncomfortable. A number of participants pointed out that AI and 'algorithms do not work perfectly, so we need a way to challenge in order to resolve errors'.

Transparency of AI systems was a critical issue for our Community. Some of the participants made it clear that they wanted rigorous analysis of each system ahead of implementation. Many felt that it should be made explicit when AI is being used to make a decision about them so that they could challenge it if need be. Some felt that disclosure is important as 'it's an ethical imperative to give consumers an informed choice'. Some wanted granular consent over what data about them can be used to inform a decision, whilst others wanted the right to opt out of automated decision making entirely. Many spontaneously called for AI and algorithms to be more regulated than at present, given the potential for negative impacts on people.

Overall, what was abundantly clear was that the consumers who participated in our Community were able to engage with the issue with ease, were able to be nuanced about the benefits as well as the risks, and had strong opinions about the retention of transparency and rights for the consumer to challenge decisions made about them.

- **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?
- **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'?

Which? agrees that, as currently written, Article 22 UK GDPR is uncertain and relates to a very specific area of 'solely automated decision making'.

We believe that there is an opportunity to extend the scope to enable the right to challenge any decision made either solely by automated means or where the use of AI is partly in the

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

decision making process. Such an approach would evolve with the development of AI, and enable a clearer framework and set of regulatory guidelines for the next steps of our AI future. It would also help keep pace with developments on groundbreaking regulation outside the UK, for example in relation to the proposed EU Artificial Intelligence Regulation that focuses on 'high-risk' AI use, bans manipulative practices and requires greater transparency.

The frequency of high-risk decisions based on consumer data continues to grow; this includes financial decisions, health decisions, decisions about access to services and decisions that can determine a contract. The right to understand and challenge these decisions will be vital. Not just for a fair society, but to ensure that decisions don't lead to unintended consequences and harms for individuals or groups, such as consumers being locked out of services, finding themselves in vulnerable circumstances based on a decision, or detrimental impacts on health and care provision. It is notable that the case study on page 38 of the consultation document refers to the COVID 'shielded patients list', which was also the subject of complaints from individuals about its accuracy, and concerns raised by expert groups about the risks of unnecessary inclusion or exclusion.

Recital 71 makes clear that processing of data used to make such decisions 'should be subject to suitable safeguards' including 'specific information to the data subject, the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such an assessment and to challenge the decision'. Our concern is that as these safeguards are not clear in the regulation, they are often not guaranteed to be undertaken.

Specific information to the data subject is often missing or poorly explained and hidden in lengthy terms and conditions, meaning that if a consumer is unclear that a decision is automated, the right to human intervention isn't sought. The right to obtain an explanation of the decision reached is hampered by AI that is hard to test (for bias, for unfairness, for inaccuracies, and simply for 'bugs'), making the decisions unexplainable not just to the consumer but anyone looking, including the decision maker. Furthermore, the data used to inform or train the AI can be inaccurate leading to outcomes that may be detrimental. For example, an error on a credit reference file can lead to a decision to deny a consumer access to necessary financial services, bank accounts, loans, mortgages or insurance. We believe that outcomes from any automated decision making needs to be verifiable and for the decision makers to be accountable.

Following the concerns expressed to us in our Community Engagement, we stress that retention of the right to challenge solely automated decisions is vital. This should also be extended to include partly automated decisions made about us.

- **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

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

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?

Which? does not support the recommendation to remove Article 22 from data protection law made in the TIGRR report.

Data provided by consumers is an integral part of products and services. Business access to it is critical for innovation and growth, but access at the expense of clear and balanced engagement with the user - be it in terms of privacy, security, autonomy or fairness - is not morally or ethically acceptable.

If the use of AI and solely or partly automated decisions are to become the norm, it will become more, not less, critical for consumers to be able to understand and challenge how decisions are made about them and seek review if they feel a decision is unfair.

We disagree with the premise in the TIGRR report that checks and balances are inhibitors to innovation and growth. We believe that clear guidelines that take both business needs and consumer rights as equal are absolutely necessary. The concept that legitimate or public interest is all that is required is disingenuous and fails to acknowledge consumer rights. Errors or misuse of data in systems and processes can be common and lead to wide-ranging unintended consequences and consumer harms.

- **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.

Building trust in data-driven systems relies on data subjects, whether they be individuals or groups of individuals, having confidence in the technology and processes being used to protect all collected data. This is especially true when considering data that may be used for profiling - with its associated potential for impact on the individual.

The key technologies and techniques that will typically be employed in the protection of data, and the identification of the data subject, are those that provide the ability to disguise or remove identifying components from the associated data, for example techniques such as synthetic data or differential privacy[8]. Data protection will typically be provided by the use of technologies that encrypt or pseudonymise data to enable it to be worked with in a way that

[8] Government Statistical Service, Privacy and data confidentiality methods: A Data and Analysis Method Review (DAMR), December 2018

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

hides a data subject's identity. This also has the potential to protect a data subject from the risk of re-identification should the data set be combined with other data. These technologies are not, at present, routinely used or understood by non-specialists. Public trust in these technologies would require that clear descriptions of their intended uses are provided.

There is a clear need for government and regulators to raise awareness further and require organisations to provide advice about how anonymisation (encryption) and pseudonymisation are applied and how they protect data.

- **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).

Which? welcomes the work that is being undertaken to develop thinking around public scrutiny of automated decision making. It will be vital to ensure systemic scrutiny of automated decision making (by data scientists) in order to enable public scrutiny. The two are different, but may employ some of the same principles and techniques. To enable public scrutiny, there should be a requirement on any businesses implementing automated decisions to make details about their training data, test data and results available.

Transparency around training data: what data is used, how much data, the completeness of the data set and so on, will enable others to form opinions about the validity of the AI and, therefore, of the 'decision'.

AI performance: how successful the AI is when run with a test data set will enable others to form opinions around how successfully the AI operates and therefore how far to 'trust the decision'. For example, in a predictive model, results of tests show data scientists how well the model performs. Tools such as confusion matrices show how well predictive models 'predict'. It is very rare for predictive models to perform at 100% accuracy.

Transparency around the use of a specific AI / Machine Learning (ML) model: how often the model is used, the range of decisions it makes, how many consumers or citizens have 'used' the model, when it was made, when it was tested and by whom, would ensure that businesses using AI were held more accountable for the AI they use. A requirement on businesses to publish such information would give consumers information they need to form an opinion about how much they trust the service. For example, models that were created or tested years ago, may be deemed less trustworthy.

Transparency around purpose and business benefit: If businesses were required to report *why* they are using AI (or ML), consumers would be able to understand the context and

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

could better form an opinion of trust (of a particular service). This may take the form of publishing a rationale statement, which could be similar to, or contained within, a Data Protection Impact Assessment (DPIA).

It is clear from our Community Engagement that consumers want to understand how decisions are made about them. Explaining how data is used, how data can be combined, how inferences are made and how decisions are reached will not only improve understanding, but will drive trust and will support the ability for consumers to be able to challenge and seek redress if required.

- **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.

Which? agrees with the ICO that the use of AI is increasingly making automated decision making mainstream and that a UK GDPR approach remains relevant, including extending Article 22 beyond solely automated to partly automated decision making. Human review must still be provided at scale, based on better training and knowledge of AI and fundamental principles of data protection. As highlighted above, given the serious policy challenges involved, there is also a need to develop specific regulation on AI as currently under discussion by the EU, especially to deal more effectively with risk assessment and transparency of AI systems, and banning of specific manipulative and harmful practices.

- **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?

Which? welcomes the proposal to provide clear and transparent testing to determine whether or not data is to be considered anonymous and outside of data protection legislation.

There is still a great deal of misunderstanding about what 'anonymous' means. This lack of understanding is highlighted by the fact that it is entirely possible to be reidentified with only three pieces of 'anonymous' information.

We would welcome therefore an expansion to the proposed testing to cover the distinction between anonymous and pseudonymous data and to clarify this for all parties. The more we can educate innovators and consumers about what these complex terms mean in practice, the better.

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

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Which? believes that using Recital 26 UK GDPR as the basis for legislative text would seem to provide a pragmatic, and familiar, form of words for inclusion in legislation. This approach is also adopted by the current ICO Anonymisation Code, which should be familiar to all UK organisations.

Great care must be taken, however, to ensure that the language used is clear and unambiguous to both professional organisations and the data subjects. For example, terms such as 'all means reasonably likely to be used' - when talking about re-identification possibilities - should not be left for individuals (organisations or data subjects) to decide on the meaning.

Also, words should not be watered down to remove the fundamental distinction between anonymous and pseudonymous data - i.e. that anonymised data has been rendered anonymous in such a way that it destroys any way of identifying the data subject (anonymisation cannot be reversed) and that pseudonymised data allows for some form of re-identification, no matter how unlikely or indirect (pseudonymisation can be reversed).

- **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)?

Which? believes that organisational confidence in the use of anonymisation and pseudonymisation could be aided by the proposal to clarify and assert that the ability to re-identify data is relative to the means available to the data controller to undertake such re-identification. However, the test of relativity that is to be applied is fundamental to the success of this and should be very carefully defined. Merely assessing what is 'reasonably likely', without clear definition, is subjective and would allow too much 'wiggle room' for organisations to the detriment of the data subject. As emphasised by the ICO[9], ongoing due diligence is also required as tools, information and options available may change over time.

- **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.

Privacy-enhancing technologies, irrespective of their complexity, provide protection of the privacy of personal or sensitive personal information. As we believe privacy to be a fundamental right for UK citizens, the responsible use of privacy-enhancing technologies should be supported and promoted by the government.

The use of privacy-enhancing technologies should be demystified and pragmatic advice provided, such that use of these technologies becomes a default in the fight against privacy abuse.

[9] ICO - Response to DCMS consultation: "Data: a new direction", 06 October 2021,

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

- **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?

Which? is following the development of data intermediaries closely; for example, in relation to the development of Smart Data projects that will focus on services for consumers.

From what we understand, widespread adoption of data intermediaries or 'trusted third parties' - for example in the form data trusts, data fiduciaries, data cooperatives or data unions - is yet to occur. Clarity on what constitutes lawful grounds for sharing of data, what the processing rights and responsibilities for an organisation of this kind should or could be, what legitimate interest and balancing tests there are and what consent mechanisms will be necessary, are therefore all open for discussion and debate beyond this strategy.

The one thing that is clear, though, is that the type of data, and the potential uses for the data, are key elements to the conversation: and there is no one-size-fits-all approach. Genomics England is a good example of what is, to all intents and purposes, a data intermediary already in action. The data that Genomics England 'manages' is specific and has specific and limited uses. It is clear to the data subject what data they are agreeing to share about themselves and their family to the project. How the data will be used is clearly explained. There is no doubt that the data subject knows what they are consenting to.

However, should a data intermediary be established for an entire sector, the data collected and then 'stewarded' is likely to be greater in volume, more complex, and the potential uses are likely to be multifaceted. The need for a balancing test for who, what, where, when and why the data should be granted access to will therefore be vital. A coverall of legitimate interest could lead to data being used for purposes that exceed data subjects' expectations, removing the necessary balancing act that would ensure business *and* data subjects are benefitted, rather than one over the other.

For consumer facing services and data intermediaries to flourish and bring societal benefit, consumer trust will be critical. Key components of that trust will be transparency, choice, control, consent, accountability and redress.

With regards to the potential for personal management systems, this is an area that could have real benefit for consumers to manage and control access to personal data. Yet, despite over a decade of investment of a range of start up innovations (including hardware, online dashboards and software applications), we are yet to see a model that has had widespread impact or uptake and which succeeds in actually putting the user in control over how data is used with whom and with what meaningful privacy and security controls and protections.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Which? welcomes the intention and wants to see strong, clear and easy to use systems that enable data portability and greater control of data to thrive. The management of data should not be an arduous, expensive, time-consuming or complex task for people to engage with.

It is worth noting that we asked our Community Engagement participants about the option of having a 'trusted third party' as a means of managing cookie consent. The response we received was that people didn't really understand what a trusted third party would be or how it would work. This was telling. There is clearly a great deal of work still to be done in relation to data intermediaries across the spectrum, be it useability, scale, purpose, development of trust, clarity on governance and many questions around liability. This is a naescent area and we will follow the plans as they develop.

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

- **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'?
- **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'?
- **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'?

Which? strongly believe that a strong data privacy framework is essential for demonstrating accountability and compliance with the law, improving privacy maturity and creating a positive data culture. The Accountability Framework in Article 5 UK GDPR provides organisations with an appropriate starting point to assess their current state of compliance.

We do not agree that there should be a general shift to a less prescriptive 'Privacy Management Programme' based on a more subjective concept of risk. In this respect, Recital 39 UK GDPR is critical because it emphasises the principles of accountability from the perspective of data subjects. It should be easy for data subjects to understand how data concerning them is processed and to get information for this reason. The requirement to have a Data Protection Officer is therefore vital. Introducing more 'flexible' and risk-based systems is not going to be easily understandable and accessible to those who are worried about the collection, retention and processing of their personal data.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

- **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'?
- **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?

Which? believes that it is vital that DPIAs are retained. We agree that DPIAs are 'helpful in the identification and minimisation of data protection risk to a project'. Undertaking a DPIA when assessing high risk processing can bring wider insight and flag areas of risk that may otherwise have been missed.

Furthermore, DPIAs offer organisations and the dedicated individuals with specialist knowledge and experience in data protection who are responsible for DPIAs, a formal and uniformed process when reviewing processing activities. The removal of the requirement for DPIAs and allowing organisations to adopt different approaches for assessing data processing and risk, may result in inconsistent practices, commercial rather than compliance-led decisions and lack of scrutiny when such assessments are carried out. We therefore disagree with the proposal to remove the requirement for organisations to undertake DPIAs.

- **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?

Which? understands that the requirement of record keeping can be burdensome on businesses and can at times feel like a box-ticking exercise. However, record keeping is vital for transparency and oversight purposes. Furthermore, once a record is in place, this can assist with monitoring and risk assessing any new activities, ensuring privacy notices are reflective of the actual processing undertaken by the relevant organisation, understanding where data is held, why and for how long, and for aiding consistency in the way data is processed. Record keeping is therefore essential for the purposes of ensuring that data subjects can enforce their rights in the event of a complaint and issues raised by consumers are addressed.

The strategy asserts that removing Article 30 requirements would only be a 'minimal' risk to effective enforcement, but presents no evidence as to why this is the case. Without a formal record of processing activities, we question how organisations can justify that their processing is lawful and demonstrate compliance with privacy laws and the accountability principle.

- **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?

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Which? does not agree that the threshold for notifying personal data breaches to the ICO under Article 33 should be reduced. Which? believes that ensuring trust and confidence in the effectiveness of data protection legislation is critical, especially given the increasing prevalence of cyber crime and concerns about insecurity of data.

Which? believes that data controllers should continue to be required to carry out internal assessments on whether there could be a risk to the rights and freedoms of individuals based on the nature of the processing of data and what data is being processed and comprehensively log data breaches. If a risk is identified the requirement to take steps to alert the relevant individuals must continue.

Furthermore, Which? believes that there should be continued support for the dedicated ICO helpline that provides advice for organisations, and further improvement and development of the guidance relating to what is and is not reportable. Such an approach would allow organisations to make confident judgements, which would in turn provide greater clarity for data subjects. Article 33 UK GDPR provides that the 72 hour deadline only applies 'where feasible', the ICO could provide more reassurance to data controllers on this point by way of practical examples. Overall, we believe that strong internal controls and risk assessments, together with clear guidance on reportability are critical tools which should be retained, and where possible strengthened.

- **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?

Which? does not agree that elements of Article 30 are duplicative or disproportionately burdensome, rather we think that it is a useful business tool and along with record keeping demonstrates good practice. While the benefits to the data subject may only be indirect, requiring organisations to be clear on the reasons why they are collecting and processing personal data enables greater transparency and understanding of how and why personal data is being used.

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

As an organisation, Which? is a data controller and as such is responsible for processing requests for access. It is our view that individuals should have easy access to their data and organisations must be encouraged to continuously improve their systems and processes in order to remove any barriers for providing personal data back to individuals. However, the ICO could be asked to consider providing additional guidance to smaller organisations if they are faced with mass requests (for example via commercial claims management companies) that are clearly vexatious and unjustified.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Which? believes that access to personal data is a fundamental right and there should be no barriers for individuals to exercise this right. Whether it is to understand how their data is being used, whether it is to find out how decisions about them have been made, or to understand whether they have missed out on opportunities, this right also promotes transparency and builds trust between individuals and organisations. Organisations cannot penalise data subjects because they have received requests from other subjects at the same time - workload or other time-consuming requests should not adversely impact any data subject, especially where their request is genuine.

- **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'?

Which? believes that the right for a data subject to access data held about them should be retained. While there are likely to be a number of data subjects who may abuse the right, the actions of the few should not undermine this. Assessing whether a subject access request (SAR) is 'manifestly unfounded' is somewhat subjective and could lead to bias in the decision making process as to whether a SAR should be rejected or not.

Clearer guidance on how organisations could better manage 'manifestly unfounded' SARs would therefore be useful. Clarity could be provided to better guide organisations to understand the context in which a SAR has been made, assess its intention and enable them to make a firm judgement whether it is or is not unfounded or vexatious.

Similarly, we think there could be value in developing further the existing ICO guidance[10] to provide greater clarity for the data subject about what constitutes a reasonable request, this may help ensure that excessive or vexatious requests are reduced.

- **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?

Which? believes that the introduction of a cost limit is unnecessary and would be detrimental to data subjects. Furthermore, any amendment that led to a reduction in the requirement to fully respond to a SAR would fail to protect the right to access and would only serve in reducing transparency and keeping people further away from access to, and understanding of, how the data they share is being used, when, how and by whom for what purpose. We do not support any reduction in the threshold for response.

- **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)'?

[10] ICO - Preparing and submitting your subject access request

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Which? wants data subjects to continue to have the right to access the data held about them. Any attempts to keep people at arm's length or to diminish transparency of data about them undermines government's intention to put people in control.

We are supportive of consumers continuing to have unrestricted access to their data. If the charge were introduced it should not be a mandatory requirement and organisations should choose whether or not to levy the charge, furthermore we would expect there to be consideration given to those unable to pay a fee so that access to data about them can still be requested and received.

From an operational perspective, the introduction of a fee would also add an administrative hurdle: the organisation would be required to set the data subject up as a supplier, cost centres would need to be assigned, payment methods would need to be determined, etc. While large organisations may be able to do this with ease and at limited cost, it would place unnecessary burdens on smaller businesses that could impact the ability to respond to a SAR or would require them to charge a higher fee if the fee was not capped.

Furthermore, the data subject would not only be required to pay, they would also be required to verify their identity. Whilst this could be an analogue process; which would involve costs to the data subject in relation to sending photocopies of identity documents, the technological direction of travel would indicate it would likely become an online digital process. With this in mind, verification of identity will require the business to undertake a digital proof of identity via digital document verification or other means such as verification of a biometric. Such an approach raises a number of data protection and security questions, particularly as there is, at present, no meaningful regulation around the use of facial and other biometrics and it remains a controversial issue.

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

Which? is concerned by the use and process of third party 'rights as a service' products offered for free that claim to help people identify which companies hold data about them and help make requests for deletion or SAR.

We are concerned about the robustness of their services and business models. These companies appear to make promises to consumers that cannot be upheld. For example, they do not appear to take into consideration an organisation's retention schedule and this results in multiple requests to erase (or seek access to) data that the organisation may not process, because of the age of that data. Such requests would require standard searching processes to be initiated - which, depending on how data is structured and where it is stored, can be time-consuming - only for there to be a nil return. This has the added impact that an organisation would be expected to retain the request and evidence of its compliance and the

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

organisation then ends up processing data on a data subject it previously did not, thereby leading to unnecessary data processing the consumer may not have wanted or consented to.

If the third party 'rights as a service' market were to expand significantly - which it is expected to - and access or other requests exercising the rights of data subjects are sent more frequently via this method, then the resulting impact on an organisation's time and resource simply would not be viable.

The ICO is clear also that where a data controller has to access a portal or agree to terms in order to view or validate a request, that organisation is deemed not to have received a valid request, yet the business models have not adapted to this and still encourage portal use.

Communication with the data subject directly is critical to this service succeeding, despite the request stating personal details are not for correspondence. As a result, many are left unverified and are not progressed and data subjects are left in the dark or frustrated.

Introduction to responses to questions relating to cookies:
To support our response to the questions relating to cookies, Which? has undertaken Community Engagement[11] with 22 consumers over 6 days to learn what they understand about cookies and what their thoughts are in relation to the proposed changes to regulation.

Hearing the voices of consumers is vital to the debate and the development of regulation. Furthermore, it provides a necessary counterpoint to the views of business. We are presenting an overview of these findings here as an introduction to the questions related to cookies. Please note, we have taken the views of the consumers into consideration in the answers we provide and the policy positions we present.

The research revealed that overall consumers want to continue to be able to actively choose which cookies are used and what data is collected about them. All but one of the participants said they were either 'not at all', or 'not very' comfortable with the idea of third party cookies collecting data without explicit consent. Indeed, 15 of the 22 participants said they were 'not at all comfortable'. We point this out not only to show that the majority of our participants did not consider tracking cookies to be essential but also to indicate the strength of sentiment. It is by no means lukewarm.

When we asked our participants to tell us which of the 4 proposals relating to cookies made by the government in the Data: A new direction strategy they felt most comfortable with:

- 13 of them felt most comfortable with setting up their choices in a browser/app/device.
- 8 of them were most comfortable with cookie banners.

[11] Which? The Consumer Voice: Automated Decision Making and Cookie Consents proposed by Data: A new direction. November 2021

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

- Only 1 wanted a 'trusted third party'.
- No-one wanted analytical cookies/performance cookies to be defined as 'essential' and collected without explicit consent.
- No-one wanted all cookies to be automatically dropped onto a device without explicit consent.

It is very clear that consumers want to continue to be able to actively choose which cookies are used and what data is collected about them.

When we dug a little further into the use of first party and functional cookies, we found that while they are seen as a little bit intrusive they were accepted as being necessary. Fifteen of the 22 said they would be 'very comfortable' or 'fairly comfortable' with data about the technology they are using (device, internet provider, time of day, etc.) being collected and used only by the first party website without explicit consent.

However, when we asked about engagement with advertising and how it can be useful, not one of the 22 respondents felt that tracking by a third party is essential, indicating that engagement with advertising is still considered to be a choice that should be made by the consumer. This matters in relation to the question of what exactly constitutes 'other similar technologies'.

The benefits of setting consent within a browser/app/device was viewed as one of convenience and ease. We were told by one participant that 'having the choice to set my device for all applications and websites would allow me to feel more in control of what data is shared'. Some questions were raised about how accessible the option would be to ensure it was inclusive and easy to use for everyone. One person wondered if users might forget or need reminding of the settings. Some felt strongly that consent should be explicit and nuanced and they were concerned the browser option may not work so well for this. In this instance, the preference was for cookie banners to be retained.

Giving the consumer the ability to consent and choose cookies remains preferable.
The view that consumers dislike or are fatigued by cookie banners is challenged by our community findings. Consumers - when they understand what the banner is asking - find them useful processes for control and choice. The problem is not the concept or inconvenience of the banner rather that there is no standardised process for how cookies are explained and how consent is presented.

- **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'?

Which? believe that the definition of analytics needs to be clear and unambiguous to avoid any possibility of it being used as a catchall for classifying any cookie or similar technology as strictly necessary and, thus, not requiring consent from a data subject.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

The ability to measure audiences and understand website performance is necessary and proportionate for a business on their website or application and reasonably falls within a clear definition of analytics. Extending the definition of analytics beyond this requires careful consideration and transparency.

For example, we have concerns about cookies and 'other similar technologies', such as tracking pixels, which are used for purposes beyond anonymised, aggregated, analytics. These technologies, which are often used together, stray into the territory of more specific tracking and profiling of data subjects' behaviours based on interactivity with advertising or analysis of behaviours for third party marketing purposes. Clearly not just measuring audiences and understanding website performance.

As clearly highlighted in ICO guidance,[12] tracking pixels have the potential to act as a marketing tool that some consumers may find interferes with their expectation of privacy, as they may be used alone or in combination with tracking and advertising cookies for invasive, microtargeting and real-time bidding purposes. Such uses go beyond the tight definition of analytics that concerns audience measurement and website performance and should therefore not be included in the definition of analytics.

Which? therefore considers it vital that the definition of analytics is clarified to cover only:

- Audience measurement where the data subject is part of a statistic and appears in aggregated and anonymised data sets only.
- Website performance.

We would expect technologies that could be used to target, monitor and/or profile a data subject to be removed from classification of analytics, be defined separately from 'other similar technologies' and be subject to explicit consent.

- **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?
- **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.

Which? is supportive of retaining the current regulation that organisations are not permitted to place cookies on websites or other technology without the consent of the individual, unless they are 'strictly necessary' for delivering an online service.

[12] ICO - Microtargeting

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

When it comes to the concept of what constitutes 'delivering an online service' we, and the consumers we spoke to in our Community Engagement, accept that making a website work is 'strictly necessary' but that monitoring, tracking or profiling users, in particular for advertising or marketing purposes, is not acceptable or 'strictly necessary'.

As noted by the Community Engagement, there remains discomfort for some that even consumer engagement analytics are too intrusive. However, there was an understanding that in restricted circumstances it can be necessary. The ability to understand website performance is important and, when undertaken correctly by a first party website using session cookies only, this should have no detrimental impact on the data subject. However, mission creep or looseness of definitions could impact this and lead to consumers being monitored or analysed in more granular ways.

Relying on legitimate interest for the narrow purpose of collecting aggregated analytics and anonymous statistics of visitors to a first party website seems reasonable so long as it is limited to that level of specificity. Broadening out in reaction to 'technological advancements' without consultation would not be appropriate.

We do not support a legitimate interest test or definitions of 'strictly necessary' for any cookie or 'other similar technology' that is able to identify a user, or that is used for intrusive tracking, targeting and profiling activities, be it by the first party or a third party website.

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

Which? does not believe or support the view that prior consent should be removed for all types of cookies. We believe this would fundamentally undermine the right for data subjects' to choose what data is collected about them, for what purpose, by whom, and for how long. It would also undermine the right to privacy and a family life.

Our Community Engagement exposed that there is an expressed desire for control and choice over how data is collected and used, which challenges the view that consumers do not want to engage with consent mechanisms.

Furthermore, any removal of prior consent would significantly diverge from cookie guidance and regulation elsewhere, particularly in the EU. Which? has concerns that this could jeopardise the EU's adequacy decision for the UK. We also have concerns around the potential for erosion of privacy rights and intrusive uses of data with no user control, particularly around profiling.

An investigation undertaken by Which? and reported as 'Can You Escape From Cookies?' in our December 2020 Money Magazine found that a number of prominent car insurer and

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

credit card company websites, as well as 'the big four' price comparison websites were failing to align with the ICO's current guidance on how to enable consumers to manage or reject cookies.

- **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?

The ability to consent via a browser/app/device settings was the preference of 13 of the 22 consumers who participated in our Community Engagement. The benefits of setting consent within a browser/app/device was viewed as one of convenience and ease. We were told by one participant that 'having the choice to set my device for all applications and websites would allow me to feel more in control of what data is shared'.

If this proposal is explored further, it will be absolutely vital however that the design, explanation and process of giving consent is clear, transparent and easy to use. A lot of users will not want to read through a lengthy policy and nor should they have to. Consumers should not be subjected to complex language or lengthy explanations. Getting the process right and ensuring the right level of detail is challenging. However, we found during our Community Engagement that it is perfectly possible to explain what cookies do easily and in a straightforward way that consumers understand and can then engage more meaningfully with. People's frustration is not with the request for consent, but with the complexity of the language and the lack of standardisation of terms used when explaining cookies, including in cookie banners.

Furthermore, if such an approach is not made easily accessible, clearly signposted and inclusive for everyone to use, consumers may miss the opportunity to set their preferred consent. This will require regulating clearly that the browsers/apps/device settings must be explicit with how they undertake the process. They must not bury or hide the process away behind complex privacy settings which require a person to click through multiple pages only to be greeted with an incomprehensible lengthy explanation and unnecessarily complex process.

Which? believes there is a benefit in exploring the browser/app/device settings option. We agree with the ICO and with our Community Engagement participants. We would like to see this option developed further and would be happy to engage with the development and testing of potential models with consumers to ensure that the design, user experience, language, signposting and ease of use fulfil consumers needs.

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

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Technologies responsible for managing the user experience/interaction (typically browsers and mobile applications) can provide an aid to reducing the volume of cookie banners, but only if implemented correctly. It is essential that these technologies honour user preferences with regard to privacy, such as 'do not track'.

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

The Consumers' Association, the parent of the Which? group, is a charity which generates its income through the commercial activities of its subsidiaries. As a charity we are 'non-commercial' and would welcome the ability to communicate more easily to our subsidiary's customers about our charitable activities. We know from member surveys and feedback that they are keen to hear about this.

However, in order to protect consumers - especially vulnerable consumers - from being subjected to spam and/or nuisance calls, it would be important that non-commercial organisations are given clear guidance on appropriate and proportionate use of the communication method. Furthermore, proportionate enforcement for rogue behaviour should be put in place, particularly with regard to unsolicited fundraising messages.

As with the commercial soft opt-in, individuals must already have a relationship with the organisation, the messages must be about similar matters to those for which details were collected, and individuals must be provided with a clear, easily accessible option to opt-out when their details are initially collected and anytime they are contacted for marketing purposes thereafter.

- **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'?

Which? is supportive of proactive, preventative approaches to protect consumers. Enabling the ICO to take enforcement action against companies, where there is evidence of poor behaviour that increases the risk of consumer harm, would be a good preventative approach to take in protecting consumers from nuisance calls.

As the ICO is already receiving reports and intelligence of bad company behaviour, there would be benefit to consumers in the ICO taking action against this, even if the incidence of harm is unclear or not particularly high due to calls not being connected.

We acknowledge that the type of enforcement action taken, may need to differ from cases where there is evidence of specific harm caused (i.e. where calls are received and connected), as opposed to an increased risk of consumer harm (where calls are 'sent' but not connected). However, we support in principle the ICO having the capability to take more

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

preventative enforcement action, the details of which we believe can be considered once the adoption of this capability is confirmed.

- **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.

Which? believes that introducing a 'duty to report' on communications providers (CPs) should offer benefits to consumers, as it is likely to enable quicker sharing of intelligence and therefore quicker response of taking enforcement action against companies causing harm to consumers.

However, enforcement action typically requires investigation, so quick blocking of the suspicious traffic would be the fastest way of offering protection for consumers. It is not clear whether CPs can autonomously block traffic that is found to be suspicious or harmful. Therefore, there is a question about whether the ICO is the right body for CPs to report to. Ofcom may be in a better position to require blocking of traffic from CPs. We would suggest CPs have a duty to report jointly to the ICO and Ofcom, or to have effective intelligence sharing processes set up between the ICO and Ofcom.

It is also not clear what the ICO will do with the reported information about 'identified suspicious traffic' and whether it will be in a position to respond in all circumstances. A lot of suspicious traffic that CPs might identify is likely to be scam traffic, as opposed to nuisance calls from companies against which the ICO could take action. We are supportive of CPs sharing data on identified suspicious traffic, but the ICO might not be in a position to act on some of those reports. We would encourage consideration of the most efficient way for CPs to share information with the relevant bodies that can then take action. As above, this could involve CPs jointly reporting to different regulators, or establishing effective data sharing processes between relevant organisations.

- **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?

There are many technological solutions that could, and perhaps should, be implemented by industry to protect consumers against nuisance and fraudulent calls and texts. However, there are also some regulatory and legislative barriers to adopting some of these protective measures. For example, CPs have regulatory service obligations which require them to deliver calls and texts to their intended recipients. This limits their ability to block traffic unless they are certain it is nuisance or fraudulent. Some technologies can block smishing messages by scanning the content of the message to check for phishing links before the

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

message is delivered, but there are questions about the legality of these solutions and whether they pose risks to consumer privacy.

While it is important to protect consumers' right to privacy, there is a case for providing clarity on the legislative barriers to these solutions. This would aid CPs in protecting consumers from fraudulent SMS traffic by giving them confidence in their ability to adopt certain technology solutions. In particular, mobile operators would benefit from relevant regulatory bodies providing clarity around how 'interception' is defined under the Investigatory Powers Act 2016. There appears to be uncertainty about whether certain technologies that scan the content of messages in an automated way without storing any data would be considered 'interception'. Clarity around this point could allow all CPs to feel confident in whether or not they can adopt solutions that could provide great consumer protection against smishing. However, we note that consideration of this issue may sit outside the scope of the regulations relevant to this consultation.

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

There is clearly benefit to consumers in taking steps to block suspicious traffic further upstream. There are different points at which consumers can be protected against harmful telecommunications, including network level (both originating and receiving networks) and device level, where protections can be built into the device or protective apps can be downloaded and installed by the user. While it is important to offer protections at different stages and levels, the further upstream the blocking takes place, the more likely it is that the calls and texts will successfully be prevented from reaching the consumer.

The risk for CPs is that they could unintentionally block legitimate traffic, which would be in breach of their service obligations to deliver calls and texts to the intended recipient. At present, CPs need to be confident something is nuisance or fraudulent traffic for them to block it. If they do not have all the necessary information to determine if it is nuisance or fraudulent, then they are likely to let it through to avoid breaching their service obligations.

Which? would be supportive of more upstream blocking at network level, rather than relying on device level blocking or consumers recognising nuisance or scam calls and texts. It may therefore be necessary to consider how to encourage CPs to block at source or to consider what information CPs need to do this confidently.

- **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'?

Which? is supportive of free of charge services that block calls that appear to be nuisance or fraudulent in nature. However, doing this based on an 'allow list' does have some limitations. Firstly, number spoofing may create challenges in this approach, as fraudsters could mimic

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

the 'allowed' calling line identifications (CLIs, commonly known as Caller ID). If the allow list is based on the CLI displayed as opposed to the originating numbers, this approach will not be effective at blocking spoofs of the numbers on the allow list.

It is also not clear from the consultation document whether the allow list will be a centralised list that CPs would consult to block certain calls at network level, or whether it is proposing blocking at device level. The question describes an allow list as 'a list of approved numbers that *a phone* will only accept incoming calls from'. The specification of 'a phone' here implies the allow list would be at device level, but it is not clear whether the blocking would occur at device level but with reference back to a more centralised list of numbers, or whether consumers would need to create their own allow lists for each device.

There are also more general limitations to allow lists. They may need regular updating to ensure traffic from new but legitimate numbers is not blocked. Nonetheless, Which? is supportive of free services to block nuisance and fraudulent calls where possible. Several CPs already offer some form of call blocking services, although these work in quite different ways and they are not offered by all providers.[13] We would like to see these services offered by default and at no cost as part of consumers' fixed line packages (with the option for consumers to opt out, rather than needing to opt in). However, we are conscious that current call blocking systems do not appear to work off 'allow lists'. We are not explicitly opposed to allow lists. We are supportive of call blocking services to protect consumers, but suggest the most effective ways of offering these are considered before deciding the best call blocking approach to take.

- **Q2.5.4.** To what extent do you think the lawful grounds under Article 6 of the UK GDPR impede the use of personal data for the purposes of democratic engagement?
- **Q2.5.5** To what extent do you think the provisions in paragraphs 22 and 23 of Schedule 1 to the DPA 2018 impede the use of sensitive data by political parties or elected representatives where necessary for the purposes of democratic engagement?

From the proposals presented in the strategy Which? believes further detail is required, particularly in relation to what 'personal data revealing political opinions' are to be in scope. If the data in scope relates to a data subject's special category data, adequate privacy measures and protections will be required so as not to undermine Article 8 of the Human Rights Act. If the personal data is to relate to a data subject's behaviour online; collected through tracking, monitoring or profiling based on advertising, targeted advertising, browsing behaviour or social media engagement, Which? opposes this data being collected

[13] Some providers have systems that work off a blacklist of numbers identified by the provider, while others operate a system that requires the caller to record their name before the receiver then chooses to pick up or ignore the call. Others do not offer call blocking, but instead offer a limited feature to simply block calls from withheld numbers. Some providers offer their services for free, although customers have to opt in, while others offer their services at a cost. This information has been gathered through engagement with the telecommunications industry as part of Which? policy work focusing on scams enabled by telecommunications.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

and used for the purpose of democratic engagement without informed consent being given by the data subject.

We have strong concerns surrounding any reduction in protections which might enable this activity to be undertaken in relation to UK political campaigning.

CHAPTER 3 - BOOSTING TRADE AND REDUCING BARRIERS TO DATA FLOWS

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

The UK's current data protection framework, which incorporates UK GDPR, is internationally recognised as being world-leading in the protections it offers consumers both domestically and when their data is transferred into other jurisdictions. Which?'s research in its National Trade Conversations has highlighted that consumers are concerned about the potential implications for their data rights from attempts to facilitate free flows of data, and they want to continue to enjoy the same level of protection when their data flows across borders as they do at home[14]. An important part of the standard of protection consumers enjoy under UK GDPR is an adequacy assessment process that accurately identifies when it is safe for free flows of their personal data without additional safeguards.

Which? agrees that the approach should be risk-based and focused on outcomes. This approach must, however, continue to protect the rights and freedoms of UK citizens and the government must ensure that the data protection laws of the relevant jurisdictions provide protection for UK citizens.

Which? welcomes the government's attempts to improve upon current international transfer mechanisms but would like to stress that an end-goal of increased data adequacy decisions and a resulting ease of digital trade for businesses without the requirement for additional safeguards, should not dilute the high standards of protection currently upheld and required for adequacy. A risk-based approach should not be biased towards businesses.

The government's intention to 'heavily focus' on 'real-world outcomes' and give less consideration to textual comparison of another country's legal text to UK data protection legislation is concerning and requires greater clarification and detail. Legal texts alone do not ensure protection, however, they are a fundamental aspect of enforceability of rights.

Consumers should have their data rights underpinned by legislation and enforced in practice in the real world. Countries that do not have legislative guarantees of adequate protections that consumers can have recourse to, that do not have formal channels for access to redress or that do not have prescriptive enforcement powers for regulators, should not be deemed

[14] Which? National Trade Conversation Report, November 2020

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

adequate and should continue to require additional safeguards from businesses. Which? would welcome more detail on how the government would assess the 'the likelihood and severity of actual risks to data subjects' data protection rights' along with how 'this approach will account for the actual practices that materially affect international data transfers between the UK and another jurisdiction, rather than accounting for academic or immaterial risks.' The UK's data protection framework provides consumers with prescriptive data rights and legal recourse - adequacy assessments should be risk-based, but should not disproportionately focus on solely the absence of certain violations in practice. Certain risks may seem immaterial, yet a stringent data protection regime should offer transparency in regard to its protections and solutions for changes in risk level.

In August 2021, the government published a draft guidance manual and template[15] for the UK's adequacy assessment process, which offered greater clarity on the questions that are intended to guide the collection of relevant information for the assessment of a country's data protection framework (this includes the content of relevant laws and the effectiveness of relevant protections). An effective adequacy assessment framework should be risk-based - it should comprehensively evaluate all the elements that could pose a risk to an adequately high standard of data protection for UK consumers. The assessment process does not fall to the government alone and will require the expert considerations of the ICO, as set out in the memorandum of understanding between the ICO and DCMS.

The government highlights that organisations currently face challenges and uncertainty when transferring personal data internationally outside of adequacy decisions, however, the standard of the adequacy assessments process should not be lowered to allow for more positive decisions to be given. Which? agrees that greater clarification and guidance is needed for organisations surrounding the alternative transfer mechanisms and the processes available to them. Increased support from the government by simplifying existing guidance on navigating the elements of the assessment and administrative processes necessary for the use of transfer tools that businesses find challenging and uncertain, would reduce some of the aspects that make alternative transfer mechanisms onerous, impractical and costly in the absence of adequacy decisions - allowing adequacy to remain an indicator of a high standard of essential equivalence. This would ensure safe transfers of personal data for consumers, who benefit from the trade in goods and services facilitated by them.

Which? agrees that the UK's approach to adequacy should appropriately account for the duty of governments to keep their citizens safe, however, this should also be proportionate. The onward transfer of data and the relationship between security measures and privacy rights are both crucial components of adequacy, which the recent invalidation of the EU-US Privacy Shield (also applying to the UK) in the Schrems II judgment reinforced. The Schrems II judgment did not change the legal criteria for adequacy - it clarified the high standard of the existing criteria. National security, public interest, law enforcement requirements, and other

[15] UK Government, Department for Culture, Media and Sport, Data adequacy: Manual guidance, Data adequacy: Manual template

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

derogations from and limitations on the protection of personal data, should be limited to what is 'strictly necessary' and consumers must have the right to effective judicial protection.[16] Any comprehensive risk-based adequacy assessment framework employed by the UK should not weaken this high standard in order to give positive adequacy decisions. Consideration should be given to governments' actions taken to keep their citizens safe but if this exceeds proportionate intervention and interference with consumers' personal data protection, those jurisdictions should require alternative transfer mechanisms and additional safeguards. The Schrems II judgment upheld the validity of Standard Contractual Clauses (SCC) in the absence of an adequacy decision - a primary alternative transfer mechanism - and imposed a stricter requirement for reviewing whether SCC actually delivered adequate levels of protection, on a case-by-case basis. The government has highlighted that businesses report finding this an onerous and complicated process requiring significant technical expertise. Which? is in strong support of greater practical support, guidance and simplification of this process that improves ease of use for businesses while ensuring adequate protection for consumers.

The government has expressed that it wishes the UK's adequacy assessment framework to inspire trust and confidence of individuals, organisations and international partners. Upholding a high standard for proportionality regarding state interference with personal data protection is a vital part of achieving this. An important aspect of this is ensuring that if this high standard is not sufficiently met to grant adequacy, the alternative transfer mechanisms available, such as SCC, are effective in delivering adequate protection in that jurisdiction which consumers and businesses can rely on. Which? is also aware of the ICO's recent publication of its draft International Data Transfer Agreement (IDTA) and guidance for organisations, which are intended to replace the current SCCs once finalised.

- **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?

Although a group of countries may share some harmonised data protection standards, or may adhere to a common multilateral framework that underpins data sharing, this alone does not guarantee that their data protection frameworks are individually sufficiently equal in practice to be deemed adequate under an umbrella decision.

For example, recent multilateral trade agreements have chapters on digital trade that contain general commitments on the protection of personal data in order to facilitate data flows without guaranteeing the same level of protection in the jurisdictions of the signatories. The United States-Mexico-Canada Agreement (USMCA)[17] deems voluntary undertakings by businesses relating to privacy to be on equal footing as comprehensive privacy, personal information or personal data protection laws. Voluntary measures would

[16] Paragraph 176, Schrems II: Court of Justice of the European Union's judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems
[17] Trade Agreement, United States-Mexico-Canada Agreement

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

not offer consumers the same uniformed protection as mandatory requirements enshrined in the UK's domestic data protection framework.

Some similar provisions are also present in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)[18], which the UK would like to become a signatory to. The provisions regarding each partner country's legal framework for the protection of personal information only recommend taking into account 'principles and guidelines of relevant international bodies', 'recognising that the Parties may take different legal approaches to protecting personal information' (Article 14.8.2).

Japan, a signatory to CPTPP, currently has a rolled-over adequacy decision from the UK from the adequacy decision given by the EU. Whereas the Australia-Singapore Digital Economy Agreement (DEA)[19] (between two other CPTPP signatories) specifically refers to APEC Cross-Border Privacy Rules[20] and the OECD Guidelines on Protection of Privacy and Transborder Flows of Personal Data[21]. Both are more limited than current UK data protection rules and are weaker in the protections they offer, with APEC being a self-regulatory regime.

Allowing for self-regulation to be on an equal footing to the comprehensive data protection regime as currently exists in the UK is detrimental for UK consumers who enjoy higher protections and could see these reduced when their data is sent abroad without adequate safeguards. This shows the significant contrast of the legislative approaches that can exist between members of the same multilateral agreements, highlighting that this does not automatically equate to uniform data protection.

In order to make regional or multilateral adequacy decisions the government would still need to investigate and conduct assessments on an individual basis. Simultaneous assessment of different countries within common regions or multilateral frameworks would require significant resources. All elements of an individual adequacy assessment would need to be satisfied with the same due diligence for each country within the multilateral framework in order to ensure consumers can continue to trust that all adequacy decisions are equal in signalling 'adequate' protection of consumers' personal data.

Questions also arise regarding the capacity for the ICO to effectively play its role in multilateral assessments. Additionally, given the temporal dimension to adequacy and the ongoing monitoring requirements, greater clarity is needed from the government as to how such proposals would address dynamic changes to individual jurisdictions within an 'adequate region' and how this would affect the collective adequacy decision.

[18] Trade Agreement, Comprehensive ad Progressive Agreement for Trans-Pacific Partnership (CPTPP)
[19] Trade Agreement, Australia-Singapore Digital Economy Agreement
[20] Text, APEC Privacy Framework
[21] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

As highlighted by the government, textual comparison of data protection regulation alone is not sufficient for an adequacy assessment. Which? believes this would be a particularly important factor in multilateral adequacy. Other elements such as the rule of law in action, respect for human rights and fundamental freedoms, and the existence and effective functioning of a regulator may vary considerably despite general binding commitments between countries. These would need to be assessed on an individual basis. An example of the complexity of the interrelation of data governance and geopolitical factors is the aforementioned invalidation of the EU-US Privacy Shield and Canada's continued rolled-over UK adequacy decision post Brexit, while both the US and Canada remain part of USMCA, and Canada also remains a signatory to CPTPP. Both the USMCA and CPTPP have broad binding commitments regarding personal data protection that seek to promote harmonisation and interoperability of standards.

In light of these complexities, Which? expect greater detail on how the government envisions the practical elements of multilateral adequacy assessments working to be published. In order to give an informed evaluation of how such a proposal would likely impact the protection of consumers' personal data in practice, far more detail on the assessment process, ongoing monitoring, individual and collective revocation, and the corresponding frameworks to each is needed.

- **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?

Which? views the ambition of strengthening ongoing monitoring as positive, as this is likely to increase the likelihood of detecting incremental changes to a country's data protection framework that may affect the handling of consumers' personal data in practice. However, from the initial proposal it is not clear exactly how the government intends to do this. Clarity on what exactly would the 'investment in ongoing monitoring of countries' relevant laws and practices' include, and how this would differ or supplement what the government should already be doing under its current obligations to monitor countries that have been deemed adequate on an ongoing basis is needed. Which? looks forward to seeing more detail on this, particularly on resourcing, capacity and prioritisation of focus areas.

At present, the Secretary of State for Digital, Culture, Media and Sport (DCMS) is under a duty to monitor, on an ongoing basis, any significant developments in an adequate country and to review adequacy regulations at periodic intervals of no longer than four years. Although some changes to the current review period may be beneficial to the government, Which? would caution against a complete removal of a periodic review deadline.

There are many dynamic elements to a third country's political system, economic development and regulatory frameworks that can significantly shift in a short period of time or that can undergo incremental changes over a longer period of time that ultimately

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

constitutes a significant enough change to how consumers' personal data is protected. The UK must have robust frameworks in place to be able to detect and assess whether a country's data protection system is no longer essentially equivalent in the level of protection of personal data transferred from the UK, and therefore requires revocation of the adequacy decision or the introduction of additional safeguards. This robust framework must include a strong incentive for third countries to maintain the aspects of their data protection system that make it adequate.

A hard periodic review deadline incentivises a third country to actively refrain from deviations and evaluate its system of personal data protection against the high standards set by the UK in order to successfully go through reassessment and maintain an adequacy decision. The adequacy assessment process is rigorous, as highlighted by the government's guidance manual. Ongoing monitoring is vital, however, it may not be possible to continuously sustain the same level of rigour as an initial assessment due to factors such as capacity, resourcing and other elements. The government highlighted the need for the UK to be able to prioritise its activities to keep pace with global developments and make new adequacy regulations. As such, a periodic deadline allows for deeper assessment that can highlight developments that may have been missed in ongoing monitoring.

At present the UK's adequacy decisions based on UK GDPR are internationally respected and denote high data protection standards, meaning that data transferred to the UK can safely be transferred with relative ease to countries with an adequacy decision, which both consumers and businesses benefit from. In order for this to continue, and for the government to realise its ambitions of being a leading hub for international data flows, the high standard of adequacy decisions must be guaranteed through re-assessment required on a periodic basis.

- **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?

Which? welcomes the government's proposal to amend the provisions of UK GDPR that govern redress mechanisms in order to give greater clarity and certainty to consumers and organisations. Clear channels of redress are vital; both across borders and in the UK. The standard that determines the requirements of an adequate or essentially equivalent redress mechanism in other jurisdictions, which would facilitate international data transfers without additional safeguards, is determined by the standard and the functioning of redress mechanisms in the UK.

Consumer access to effective redress mechanisms is a priority for Which? We submitted a response to the government's Call for Views and Evidence for the Review of the Representative Action Provisions in Section 189 of the Data Protection Act 2018 (DPA) in

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

2020[22]. Which? is seeking the implementation of Article 80(2) UK GDPR which would introduce the redress mechanism of representative action without the specific mandate of the data subject for consumers. Access to adequate redress is a necessary consumer right and vital part of a robust data protection framework; there is a compelling need for better provisions.

UK GDPR currently outlines redress mechanisms and remedies in a number of separate articles. UK GDPR gives effect to the right to both effective judicial remedy and provides for administrative mechanisms, however, there is ambiguity surrounding the exact nature of those administrative and judicial remedies which may benefit from greater clarity. There are also optional redress elements that were at the discretion of the government to implement during the time of transposition of the legislation that in Which?'s opinion require review and extension.

Currently, UK GDPR gives data subjects the right to an effective judicial remedy against a data controller or processor in Article 79. The legislation also gives consumers the right to claim compensation if they have suffered damages as a result of an organisation breaking data protection law. This is a judicial redress mechanism, the ICO cannot award compensation directly to consumers at present. This right to compensation and the imposition of liability in this regard is governed by Article 82 UK GDPR which includes compensation for material and non-material damage.

Consumers also have recourse to administrative redress mechanisms, Article 79 states that the right to judicial remedy exists without prejudice to any available administrative or non-judicial remedy. Data subjects have the right to lodge a complaint with the ICO according to Article 77. The ICO can fine organisations following certain breaches of data protection law. Article 83 outlines the general conditions for imposing administrative fines. The DPA outlines other enforcement tools (enforcement, information, assessment and penalty notices) available to the ICO to remedy non-compliance or violations of data protection rights.

The government chose not to implement Article 80(2) which would have allowed not-for-profit organisations meeting certain criteria to bring representative actions (judicial or administrative) on behalf of consumers without them having to appoint the organisation themselves, or without each data subject affected having to individually 'opt-in' to an action started.

A robust redress framework should provide for both administrative and judicial mechanisms, should be clear regarding what they are, and perhaps most importantly, should be able to be used by consumers with relative ease. In order for the government to achieve its intention of advancing digital trade by facilitating 'trusted cross-border data flows', it must deliver

[22] Which?, Response to the Call for Views and Evidence for the Review of the Representative Action Provisions in Section 189 of the Data Protection Act 2018

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

effective administrative and judicial redress mechanisms for UK consumers domestically. Third countries' redress frameworks can then be evaluated against these for suitability for cross-border data transfers and adequacy.

Which? strongly believes that an effective domestic data protection redress framework requires a collective redress mechanism on an opt-out basis to be introduced for violations of data protection law, including significant data breaches. This would aid in creating an environment where data subjects have confidence in the way that organisations are using their data and are assured that there are processes in place to protect their data rights if something goes wrong domestically or internationally.

The current 'opt-in' redress system is not working to adequately serve consumers who suffer at the hand of data breaches and business practices that breach data protection principles. This is evidenced by the low uptake of the current provisions, highlighted by both the government and the ICO in its statutory review process. A major barrier to the uptake of the current redress mechanism is that it places a heavy onus on consumers and does not account for hurdles. In the case of data breaches for example, the current model presupposes that affected consumers are aware that their data has been breached, that they know their right to appoint a representative body, and that they see the value in expending time on such an appointment in circumstances where the individual harm suffered may seem relatively small even though it may have had a much greater aggregate cost and collective impact on consumer welfare.

Which?'s reference to opt-out collective redress includes the regulator taking action in respect of a complaint, seeking a court order requiring a data controller or processor to comply with data protection legislation, judicial remedies against supervisory authorities and compelling measures for companies. However, in our view, an effective judicial remedy against a controller or processor should also include compensation.

Large scale infringements of consumers' data rights continue to happen with consumers suffering real harm as a consequence but without having access to the redress mechanisms they deserve - administrative or judicial. Multiple high-profile data breaches have occurred in the years since the introduction of the legislation. Which? has published investigations that showed the real-life impact these can have on consumers' lives. The recent high profile decision of the Supreme Court in the case of Lloyd v Google[23] illustrates clearly that the current options for collective redress for consumers in data protection cases are too limited, letting large companies off the hook for non-compliance. It should therefore be a priority for the government to review their position and to take action implementing Article 80(2). In this way, opt-out collective redress mechanisms can be provided, with the appropriate safeguards, as in cases brought under the Competition Act 1998.

[23] Judgment, Lloyd v Google [2021] UKSC 50

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

More needs to be done to hold organisations to account when they do not adequately protect consumers' data or engage in business practices which contravene the UK's high data protection standards - more needs to be done to incentivise them to improve their data processing practices. Facilitating redress through an opt-out mechanism would be a complementary method to incentivising good practice alongside existing measures. It would reassure consumers that the high standard of protection that governs their personal data is backed by tangible and accessible recourse should their rights be infringed domestically or when transferred internationally. This is an opportunity for the government to be at the forefront when it comes to facilitating trusted international data transfers underpinned by effective redress mechanisms for administrative and judicial remedies.

- **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?

Alternative transfer mechanisms facilitate the cross-border transfer of consumers' personal data to countries that do not have an adequacy decision. These transfer mechanisms ensure appropriate protection for consumers' rights and freedoms in respect of their personal data when it is transferred to those jurisdictions. It is important to remember that the aim of these mechanisms is to facilitate international transfers by adding safeguards and mitigating the risks in environments that have not been recognised as having sufficient safeguards of their own that meet the standards of the UK's domestic data protection regime.

The government proposes reinforcement of the importance of proportionality when assessing risks for alternative transfer mechanisms. Proportionality considers that in pursuit of an aim, only necessary actions are taken that do not go beyond what is needed. In the context of risk assessments for alternative transfer mechanisms this is a complex issue as proportionality should not be interpreted as the bare minimum. Although assessing risk can be challenging and time-consuming for organisations when deciding which transfer mechanisms can be used, thorough risk assessments are a vital part of providing binding and enforceable protections. A proportionate risk assessment process should not be excessively onerous and challenging for organisations, but they should also be carried out with sufficiently high scrutiny, as data controllers will be held accountable for their choice of alternative transfer mechanism in practice.

While it is important to ensure that the safeguards applied to international transfers of personal data are proportionate to the risks to consumers' personal data, and while cross-border data flows are important to a functioning economy, consumers' personal data should not be left unduly exposed to lower standards of protection in other jurisdictions due to disproportionate changes to the risk assessment process. A proportionate approach to risk assessments should still adequately account for laws, enforceability of rights, practical elements and redress mechanisms and should highlight when supplementary safeguarding measures are required in addition to the alternative transfer mechanisms.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Which? agrees that much more support and guidance is required and welcomes more detailed, clear, practical support for organisations on determining and addressing risks, particularly for smaller organisations that lack the resources for significant technical expertise.

The Draft International Transfer Risk Assessment Tool ('DRAT') that the ICO recently published with its consultation on International Data Transfers under UK GDPR is a positive development. However, more guidance is required, particularly where the transfer is a higher risk, as the DRAT seems only to apply to lower risk scenarios. The DRAT presupposes that the organisations using the assessment have the ability to assess whether the data transfer agreement will be enforceable in the third country or understand how the country's specific legislative regime may allow for surveillance of such data. The DRAT is helpful for providing guidance on how to assess the transfer, what considerations to make, what may constitute higher risk data and how to supplement the safeguards already provided for in the draft international data transfer agreement.

Which? would welcome more guidance from the government in how the government would assess the risks posed by data protection regimes in any third countries and how this would link to the proposal to reinforce the importance of proportionality.

- **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?

Although the international data protection landscape is evolving and the ways in which organisations use data will continue to develop, Which? believe that the standard of data protection UK consumers can expect, and the legislation which underpins this, should remain clear and uniform. Although Article 46 UK GDPR at present includes an exhaustive list of the types of alternative transfer mechanisms at the disposal of data controllers, they provide for some flexibility.

The current alternative transfer mechanisms can be added to within their type if approved by the ICO following the necessary processes for each tools' framework. For example, the ICO can create new certification schemes according to its criteria if future developments necessitate this, which would then be issued by accredited certification bodies. Certification will relate to specific personal data processing operations that take place in products, processes or services offered by data controllers or processors. These certification schemes can, under certain conditions, be used to demonstrate the existence of appropriate safeguards provided by controllers or processors that are not subject to UK GDPR for international transfers of data according to Article 42(2) UK GDPR.[24] Additionally, the fixed

[24] ICO, Certification Guide for Organisations

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

set of transfer tools outlined can be amended through legislative proposals, such as those that the government is currently consulting on.

Which? is supportive of the ICO's work towards offering greater clarity and support for organisations to make better use of the existing options for tailored transfer mechanisms (Binding Corporate Rules, Codes of Conduct and Certification Schemes) and the other alternative international transfer mechanisms. The government intends to explore amendments to the international transfers regime to give organisations greater flexibility in their use of transfer mechanisms, including empowering organisations to create or identify their own alternative transfer mechanisms that provide appropriate safeguards. This raises cause for concern from a consumer perspective. The UK's framework should be sufficiently adaptable to future developments in the international data protection landscape, however, it must continue to provide a uniform and consistent standard of protection.

While greater flexibility may certainly be beneficial to organisations, allowing businesses to create their own alternative transfer mechanisms could result in varying degrees of protection for consumers. More detail is required on how 'organisations that chose to create their own mechanism would determine how the mechanism meets the requirements for appropriate safeguards'. If organisations are allowed to exercise discretion regarding which requirements to adhere to, or are allowed to omit certain requirements entirely, then there is a significant risk that consumers' data will not be adequately protected. The government's proposal states that it would remove the requirement for proactive approval from the ICO, instead transparency and accountability requirements would be fulfilled by other means, such as impact assessments or 'clear documentation' of rationale to demonstrate reasonable grounds for the belief that appropriate and enforceable safeguards are in place. This raises some concern. Without proactive approval from the ICO these appear to be voluntary undertakings without sufficient oversight that would not reassure consumers of the same level of protection as prescriptive alternative transfer mechanisms. From a consumer perspective this would be a regression - without guaranteed safeguards approved by the regulator, it would introduce flexibility into a stringent data protection framework and weaken it.

The government states that organisations would be supported via guidance from the ICO. Would adherence with this guidance be assessed? Would assessment take place before a transfer mechanism was used to transfer personal data or only if a breach of consumers' data rights became apparent? Much greater detail is required on this proposal as a whole in order to begin to determine whether consumers' personal data could be protected to the same level as current data protection standards using such mechanisms.

- **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?

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Under UK GDPR, organisations are already permitted to make international transfers that rely on the protections provided for in another jurisdiction - those jurisdictions that have been deemed as providing essentially equivalent protections to those provided for in the UK's domestic data protection framework during an adequacy assessment (Article 45 UK GDPR). Alternatively, certain alternative transfer mechanisms can be used that rely on the protections provided for in the UK's domestic legislation. Both of these mechanisms for international data transfers provide assurance to consumers that their personal data is consistently protected by the same high standard.

The government has already highlighted some of the difficulties currently faced by organisations when conducting risk assessments for the purpose of determining which alternative transfer mechanisms and additional safeguards are best suited for transfers to jurisdictions without an adequacy decision, with lack of resources and technical expertise becoming barriers for some organisations. The level of technical expertise required to make an assessment of whether another country's data protection legislation offers appropriate safeguards is significantly greater. This is apparent due to the many factors that will require thorough consideration and analysis when the government is conducting its adequacy assessment of the data protection framework of another country, as highlighted by the government's draft guidance manual and template for the UK's adequacy assessment process published in August 2021. Comparing the text of legislation would not be enough to determine whether personal data is appropriately safeguarded. For organisations to have a reasonable basis to believe that comparable safeguards will be upheld in the jurisdiction they wish to transfer consumers' personal data to, they would need to carry out their own adequacy assessment of sorts. This would subvert the importance and standard of the government's adequacy decisions given to those countries that had been deemed as providing adequate protections during the rigorous assessment conducted by the Secretary of State and the ICO.

In the absence of a UK adequacy decision, data controllers or processors should only transfer personal data to a third country or an international organisation if they have provided appropriate safeguards through approved alternative transfer mechanisms, or in cases where the derogations for specific situations as outlined in Article 49 apply. This provides certainty for both consumers and businesses that adequate enforceable data subject rights and effective legal remedies are available as specified by the standard set in the UK's data protection framework.

- **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?

Which? believes that it is vital that the high standard of personal data protection that UK consumers currently enjoy, which underpins trusted cross-border data transfers made by organisations, is maintained and built upon in an evolving digital trade and international data

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

landscape. Should international developments in the digital landscape necessitate new mechanisms for safely transferring consumers' personal data across borders, the Secretary of State should be able to respond to this need by following an appropriate development and vetting process that would ensure that a new transfer tool upholds the high standard set in UK GDPR. However, the ICO should also have significant involvement in the development and oversight of any new alternative transfer mechanisms.

The government also mentions the recognition of new transfer mechanisms used by other countries or groups of countries. A stringent assessment process would need to take place to assess the compatibility of externally developed transfer mechanisms with the principles and high standard set by the UK's domestic framework. The ICO would need to play a central role in this assessment before the Secretary of State approved any new international data transfer tools. This would benefit from a statutory requirement. An increase in interoperability should not come at the cost of the high level of personal data protection provided by the UK's existing transfer mechanisms, which facilitate international data flows.

- **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?

In paragraph 270 the government proposes 'establishing a proportionate increase in flexibility for use of derogations by making explicit that repetitive use of derogations is permitted'. Repetitive use of derogations is currently restricted by the UK GDPR Recitals. Government outlines that this new permission would apply to all of the derogations except the derogation for compelling legitimate interests. Derogations are intended to apply in limited circumstances that necessitate a deviation from the normal procedure. Article 49 UK GDPR outlines specific conditions that would warrant an exception from the general rule that restricted transfers of personal data should not be made in the absence of a UK adequacy decision, alternative transfer mechanisms or appropriate safeguards being put in place. The provisions clearly indicate that the use of derogations is intended to be for exceptional circumstances. An increase in the repetitive use of derogations would mean an increase in situations where the general standard set to govern the processing of consumers' personal data is partially suppressed. A need for continuous and more frequent use of derogations would signal that there has been a significant shift in the data transfer landscape that requires assessment, alongside the data protection framework that governs them.

The government states that there would be 'certain limited but necessary situations' where repetitive use of derogations should be permitted. It would be beneficial to understand what situations the government anticipates these to be, as the use of derogations is the final mechanism available to organisations for transferring data internationally - a last resort.

The ICO's response to this consultation notes: 'Where transfers are repeated and predictable, there is an opportunity to put in place appropriate protections for people's data,

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

through the use of [an alternative international transfer mechanism] AITM. Where it is possible to put such protections in place, either wholly or in part, this should be done to ensure people are protected.' If the transfer is going to be repetitive then it is unclear why one of the existing safeguards outlined in Article 46 UK GDPR could not be adopted, at least in part, with supplementary safeguards to ensure adequate protection.

Paragraph 156 of the ICO's response to the consultation highlights that in its view there may be certain situations where a transfer is repetitive, but it is not possible to put in place an Article 46 transfer tool, and that in such instances reliance on a derogation may still be 'necessary and proportionate'. Which? agrees with the ICO's recommendation that if such circumstances should indeed arise, there should be a requirement for the data exporter to document such transfers and all necessary safeguards they have put in place to protect consumers' personal data as a minimum requirement. Which? would urge the government to consider further measures that would ensure the protection of consumers' personal data in these limited scenarios.

However, the government stated its intention for its exploration of legislative changes to the UK's framework for international data transfers is to ensure that the alternative transfer mechanisms available to UK organisations in the UK GDPR are clear, allow for proportionate flexibility and provide the necessary protections for consumers' personal data. This should reduce the need for derogations for repetitive transfers.

CHAPTER 5 - REFORM OF THE ICO

- **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?

It is an existing statutory obligation of the ICO to take into account 'the desirability' of promoting economic growth when exercising its regulatory functions under the Data Protection Act 2018 in accordance with duties under Section 108 of the Deregulation Act 2015.

The suggestion that the ICO should have this statutory duty strengthened, and also extended to include innovation, is not necessarily justified. This may risk diluting the main focus of the ICO to protect and enforce the rights of data subjects. In any event, we support the ICO's general view on the consultation[25] that any changes to further support economic growth must:

- retain high standards of protection for people's personal data;
- make sure people's data is used in ways that benefit rather than harm them; and
- make sure people can easily exercise their rights'.

[25] ICO, Response to DCMS consultation "Data: a new Direction", 6 October 2021, at p.9

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.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?

In our recent response to the BEIS consultation on Reforming the [UK] Framework for Better Regulation,[26] Which? highlighted that we do not consider it necessary or appropriate to require all regulators to have a duty to consider competition and/or innovation, as in some cases this would result in conflicting obligations that may impede a regulator from effectively discharging its primary function and public protection duties. Creating an additional duty for the ICO to have regard to competition when discharging its functions introduces priorities which may be counteractive to its purpose outlined in UK GDPR and its self-determined strategic goals.

The processing of consumers' personal data is vital for domestic digitally-enabled transactions of trade in goods and services and underpins the data flows that facilitate international digital trade. As such, there are many ways in which competition and data protection are interconnected. In May 2021, the ICO and the Competition and Markets Authority (CMA) published a joint statement on competition and data protection in digital markets, which describes the interactions between the regulators and their respective regimes[27] and makes clear that there is mutual agreement that they 'want to ensure a digital ecosystem where people have a genuine choice over the service or product they prefer, with a clear understanding of how their data will be used to inform that decision.' Which? welcomes this approach and is supportive of regulatory interventions to promote competition and data protection being productively aligned in a way that is mutually reinforcing.

However, as the government notes in the proposals, tensions can arise between actions taken to promote competitiveness within markets and actions taken to promote a higher standard of data protection, such as increasing access to personal data in an attempt to increase competition. Tensions can also arise between data protection objectives and actions taken to improve the competitiveness of the UK as a destination for international organisations to conduct their business. Environments with less stringent data protection laws and enforcement can seem more attractive to businesses that want to reduce their data compliance costs.

Tensions between competition and data protection could result in conflicting interests for the ICO if a duty to have regard to competition when discharging its duties was imposed. In the CMA's and ICO's joint statement on competition and data protection, the regulators also acknowledge that there are areas where tensions can arise between data protection and competition, but that these 'can be reconciled through careful consideration of the issues on

[26] UK Government, BEIS, Reforming the Framework for Better Regulation: A Consultation
[27] ICO, CMA, Competition and data protection in digital markets: a joint statement between the CMA and the ICO

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

a case-by-case basis, with consistent and appropriate application of competition and data protection law, and through continued close cooperation' between the two organisations.

Greater cooperation between regulators on data protection and competition is therefore vital to balance out these potential tensions rather than the imposition of a duty for the ICO to have regard to competition when discharging its duties. Consumers must be reassured that if significant conflict arises between the UK's data protection principles and external objectives for promoting competition (domestically or internationally), the ICO is able to act in the best interest of data subjects and discharge its functions without influence from a new statutory duty imposed on it.

- **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)?

We welcome this proposal and we see this as an opportunity for the ICO to assist in ensuring a level playing field and promoting fair competition in digital markets, while still protecting individual data rights as a priority.

The recent collaboration between the ICO and CMA on the subject of competition and data protection in the digital market is a positive example of the ICO and other regulators working together and aligning strategies to provide expert advice and thought leadership that can benefit both organisations and individuals. We agree with the government's proposal to endorse and further encourage such collaboration.

Which? welcomes the interaction and collaboration between the regulators. We agree that the interplay between data protection, competition and anti-competitive behaviour requires bilateral and multilateral regulatory oversight. We supported the creation of the DRCF and support the idea of data sharing, collaboration, staff secondment and training across and between the regulators. Digital platforms are multifaceted and offer a wide range of services and products that do not neatly align with one regulator.

Consumers' data is at the heart of many connected digital products and services and therefore an integral part of innovation, growth and competition. Consumers want to see more choice and competition in digital products and services, and want the reassurance that the data they provide is used appropriately. At present, choice and competition is inhibited in many areas by the fact that the largest platforms have access to the most data. Data protection is often used as an excuse as to why that is but the argument is disingenuous. Data protection is not an inhibitor to innovation, competition, growth or diversity of choice of services - it is an enabler.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

- **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?
- **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?
- **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?

Which? believes that due to the multifaceted nature of the products and services offered by online platforms and the large big tech companies, it is logical, and indeed necessary, for the regulators to collaborate and bring their specialist skills and knowledge together rather than working in isolation.

This is particularly vital when it comes to ensuring that the regulators have access to the relevant data and information when undertaking investigations regarding anti-competitive behaviour, data collection, use and breach, and the cross-cutting nature of online harms and safety. However, with any form of collaboration between different bodies, it is vital that clear parameters are defined in order that each regulatory body understands their role in an investigation or in a collaborative/cooperative environment.

Getting the balance right will be critical, as there is always the risk of too many cooks, but we are encouraged by the voluntary approach the regulators are currently taking in relation to the DRCF and the published work-plan.

Of course, the success of the regulatory bodies also rests on them having the correct, and necessary support. We welcomed the statement in the 'Digital Regulation: Driving growth and unlocking innovation' policy paper that the government 'will continue to make sure our regulators can adapt and have the right capabilities and expertise to take action effectively and proportionately'.

Which? would encourage this to include:

- staff with the right technical, ethical, data, digital, security and legal skills;
- regulators having the necessary tools, such as the ability to deliver robust oversight, auditing where relevant and needed, and tough enforcement powers to ensure the regulations are adhered to and when not that organisations and companies are appropriately sanctioned;
- the ability for regulators to be able to access all the necessary evidence, intelligence and data including from companies that sit outside of the UK but are used by UK consumers. Ensuring there are no restrictions on access to such data and evidence will be a critical element of UK trade deals; and
- the ability for UK regulators to work and collaborate with their international counterparts to ensure cross border issues are tackled appropriately.

Which? believes that:

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

- the Office for Product Safety and Standards (OPSS);
- the Medicines and Health Products Regulation Authority (MHRA);
- the Advertising Standards Authority (ASA); and
- the Civil Aviation Authority

could all be considered relevant for a duty to consult and co-operate, and should be considered as relevant for any potential information sharing gateway.

All four regulators are either currently involved in overseeing products and services which collect, store, share or interact with consumers personal data, including: connected/Smart products (OPSS), commercial medical health wearables and applications (MHRA), the oversight of online advertising (ASA) or air travel services (CAA).

- **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?

Which? is worried this proposal could undermine the ICO's independence. A primary way in which the government can empower the Information Commissioner to protect data rights and promote trust in the data protection system in order to unlock the power of data is by ensuring that it remains completely independent. Article 52 mandates that the ICO must remain free from external influence, whether direct or indirect, and must neither seek nor take instructions from anybody when exercising its powers in accordance with UK GDPR.

The Secretary of State for DCMS periodically preparing a statement of strategic priorities that the ICO must have regard to when discharging its functions could undermine the ICO's independence. This could also pose a significant obstacle to the regulator's ability to uphold and enforce the data protection framework in the best interest of data subjects.

A supervisory authority needs to be adequately resourced in order to fulfil its remit. It also needs to be able to legitimately act in pursuit of its primary objective without restrictions or fear of retribution from external parties that could significantly impact its operations.

The ICO holds significant expertise in identifying data protection issues and in identifying areas that would weaken the UK's domestic data protection framework and cause harm to consumers' data rights. The government highlights that the ICO also plays a vital role in developing information rights practices internationally using its expertise. It is that expertise that it used to develop its current six strategic goals, which it first published in its four year plan in 2017.[28]

The ICO should be allowed to continue to set its strategic goals and priorities based on its expert analysis. This does not prevent the government from making suggestions or

[28] ICO, Information Rights Strategic Plan 2017-2021

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

recommendations based on its domestic and international priorities, so long as there is no statutory duty which encroaches upon the ICO's independence.

Although the government mentions that the ICO would not be bound by the statement of strategic priorities, it would however, be expected to respond to the statement and give an explanation as to whether and how its work addresses the priorities set out by the government. This requirement is still a significant steer that incentivises compliance with the government's priorities. The government makes reference to Ofcom, Ofwat and Ofgem as other regulators who receive a similar statement of strategic priorities on how they should set their regulatory priorities. However, unlike those regulators the ICO plays a role in regulating the government and the public sector. This makes it even more vital for the ICO to be completely independent.

The ICO needs to be able to adequately assess whether government proposals across all policy areas are compatible with the UK's data protection framework and it should be able to hold the government accountable in its capacity as a data controller that processes personal data. It is important for the ICO and DCMS to be able to continue to work closely to ensure high standards of data protection are implemented effectively in the UK. This requires the ICO to be able to, if and when necessary, oppose government proposals that it deems detrimental to the high standard of data protection consumers have come to expect, even if those proposals may have beneficial implications for the government's strategic priorities in other policy areas.

The ICO highlights in its own response to this consultation the importance of independence, within a framework of strong accountability to Parliament. It allows the ICO to 'regulate without fear or favour, to make decisions about where [it] intervenes or acts based on an impartial assessment of the harm or potential harm to people'. It also 'reassures the public that its actions are impartial and that the government as well as businesses are being held to account'.

- **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?

The ICO works to uphold and enforce the high standard for consumers' personal data protection set by UK GDPR domestically and in international contexts, and in doing so facilitates cross-border data flows and digital trade. It plays a complex and important role in promoting responsible and trusted cross-border data flows through its legislatively mandated work on developing and maintaining transfer tools and its influential regulatory cooperation activities in key global fora. The proposal of a new statutory objective for the ICO to consider the government's wider international priority is therefore concerning in this context, as the government's international priorities may conflict with the ICO's strategic objectives and undermine its independence.

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Which? would like to emphasise the crucial importance of the ICO's complete independence as a regulator also with regard to its international activities. Article 52 UK GDPR is explicit - the ICO must remain free from external influence, whether direct or indirect, and must neither seek nor take instructions from anybody when exercising its powers in accordance with UK GDPR.

The government has made its intentions clear that it is strongly focused on 'exploiting opportunities' to promote economic growth through digital trade. Its ambition is for the UK to be 'a leader in digital trade and the world's most attractive data marketplace: an open, welcoming and secure destination for companies from all over the world to share data, grow their businesses and innovate across all sectors of the economy'. An important part of the ICO's role is to support the government's intention of giving consumers confidence that their personal data remains protected within this goal, and ensure that the government's priorities set in pursuit of these international ambitions are not detrimental to consumers' data rights. This requires the ICO to be able to, if necessary, oppose government proposals that it deems detrimental to the high standard of data protection consumers have come to expect, even if those proposals may have beneficial implications for the government's broader international priorities. The government's commitments to the 'reduction of barriers and burdens that organisations face when transferring data overseas', and adding more countries to the data adequacy list by 'progressing an ambitious programme of adequacy assessments' are in particular need of the input and collaboration of an independent ICO, whose international priorities are rooted in its legislative purpose. The importance of independence of data protection authorities is increasingly being recognised in the international landscape and is reinforced by agreements such as Convention 108+, to which the UK is a signatory.

The ICO has been effectively carrying out its international activities in accordance with its mission of upholding information rights for the UK public in the digital age. The ICO currently chairs both the Global Privacy Assembly and OECD Working Group on Data Governance and Privacy. One of the ICO's current six strategic goals is to 'maintain and develop influence within the global information rights regulatory community'.[29] It outlined in its Information Rights Strategy Plan that it recognises that data protection regulation has an increasingly international dimension, and that leaving the European Union presents opportunities for new or enhanced relationships with information rights regulators and communities on the worldstage.[30] The regulator has used its expertise to develop an international strategy designed to achieve global reach and influence, and has signalled its continued intention to work closely with the government in this area.

Although the ICO's international role may benefit from clearer strategic objectives against which it can prioritise its activities and resources, these should be set by the regulator following expert analysis of developments on the international landscape. The regulator

[29] ICO, Mission, Visions and Strategic Goals
[30] ICO, Information Rights Strategy Plan 2017-2021

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

should consider the impact that international developments could have on data subjects' rights, the government's priorities and, most importantly, the interaction of regulatory developments with the UK's own data protection legislative framework. Which? is supportive of proposals for the ICO to deliver a more transparent and structured international strategy as part of its accountability and transparency requirements. However, this does not require a new statutory objective for the ICO to consider the government's wider international priorities when prioritising and conducting its own international activities.

The ICO highlights in its response to this consultation that maintaining an independent supervisory authority is an important element of 'demonstrating that the UK has the high standards of data protection that the international community expect, and which will be required for future global trade deal considerations and adequacy agreements'. The ICO is capable of using its expertise, and consultation when necessary, to develop an international strategy designed to achieve global reach and influence that upholds UK data subjects' rights. It has also continually signalled its intention to work closely with the government to do so.

- **Q5.3.2.** To what extent do you agree with the use of the Public Appointment process for the new 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?
- **Q5.3.4.** To what extent do you agree with the use of the Public Appointment process for the new CEO of the ICO?

Which? is concerned with the proposal for Public Appointment of key executive roles within the ICO. Removing the ICO's autonomy to appoint members in executive positions will undermine its role as an independent regulator for the government and public sector and will result in lack of trust from organisations and the public in the UK and internationally. It is vital that the ICO continues to have this independence from government. Therefore, we agree with the ICO's response[31] to this proposal and we support the view that the ICO's Board should maintain responsibility for appointing members in executive positions.

- **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?
- **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?
- **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?

[31] ICO, Response to DCMS consultation Data: A new direction

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

Which? agrees that accountability and transparency are key mechanisms in ensuring the ICO delivers on its strategic objectives and continues to support the public and organisations in the most efficient way. The current annual report[32] produced by the ICO contains useful information about the ICO's key activities. However, we agree that this can be improved to provide meaningful and transparent reports in a data-driven world and to assure the public and organisations of the effectiveness of the ICO.

Examples of improvement areas in the ICO annual report:

- Strategic priorities - these are currently listed, but lacking details on the ICO's performance against those priorities. We welcome more detail on performance against KPIs and how they link to statutory and organisational objectives and priorities.
- Operational performance - it is very useful to see the number of complaints, SARs and breaches reported by the public and investigated by the ICO. It is particularly helpful to see the breakdown by industry sector, which shows where further guidance is needed to support organisations in those sectors to reach compliance or whether enforcement actions need to be taken. It is also useful to see the performance of the ICO and the timeframes within which these requests have been dealt with. It would be helpful in the future to include information on repeat offenders to alert the public about potentially non-compliant organisations. It would also be useful to report on the cause of breaches (i.e. human error, security error, lack of organisational control etc.) to give further context to the reports.
- Fines - the ICO also provides a brief summary on enforcement and names organisations where fines have been effectively imposed. We would like to see increased enforcement reports naming all organisations who have received fines and not just the giants. We would also welcome reports on whether those fines have been paid by the organisations. This is vital to demonstrate the effectiveness of the ICO's enforcement powers and to further build public trust in the actions of the ICO.

- **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?

Which? agrees that a consultative approach and engagement with organisations, stakeholders and people can be beneficial in the development of new guidance. It is important the ICO listens to the voices of different groups when developing new codes of practice and guides. It is equally important that businesses and individuals feel consulted and involved in the process. Often ICO guidance can be highly technical and theoretical, and organisations, individuals and groups need expert advice to interpret and understand how to implement it. A more consultative approach will bring the ICO closer to the practical aspects of data protection and will ensure that new guidance incorporates the needs of all groups

[32] ICO, Annual report and Financial Statements 2020-21

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

involved. This will further increase the value of the guidance the ICO provides and improve understanding and engagement with data across society.

- **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?
- **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?
- **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?

Which? does not agree with the proposal to give the Secretary of State the right to approve or reject guidance issued by the ICO. Which? strongly objects to this proposal as it undermines the independence of the ICO. The ICO is well-regarded domestically and internationally as the expert on data protection in the UK. The proposed change will undermine trust in the ICO.

Furthermore, we would want to see much greater detail about the proposal of a 'panel of persons with expertise'. A wide range of expertise, including technical expertise as well as legal acumen and consideration of ethics and data ethics, can be beneficial. It is vital that any 'panel' is completely independent of government, and includes consumer representatives.

- **Q5.6.1**. To what extent do you agree that the ICO would benefit from a more proportionate regulatory approach to data protection complaints?
- **Q5.6.2.** To what extent do you agree with the proposal to introduce a requirement for the complainant to attempt to resolve their complaint directly with the relevant data controller prior to lodging a complaint with the ICO?
- **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?
- **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

We acknowledge that the ICO faces high volumes of complaints every year, but note that the consultation document states that the number of complaints decreased in the past year. In addition, the GDPR has only been in force for three years and it would be beneficial to look at complaint trends over a longer period of time before jumping to conclusions about

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

legislative changes. Individuals experience issues in practice when trying to resolve their problems, and are increasingly required to go through confusing online reporting processes, particularly by large technology companies. It is therefore vital that there are no barriers to raising complaints directly with the ICO.

In addition to the safeguard of potential ICO involvement from the outset, Which? expects to see a clear and transparent complaints process outlined by all organisations which makes clear to the consumer who they can complain to, what the time frame of processing and response to a complaint will be and what course for redress they will have.

Currently, organisations are not legally required to have a specific data complaints process. Many organisations include instructions on complaints in their privacy notice. This often is not transparent and individuals are required to undertake an arduous process of navigating a website in order to find the right page, and then are required to read through an often very lengthy privacy notice in order to find the correct contact details and procedure.

Additionally, organisations can have different approaches to handling data complaints based on many factors, such as how mature they are in managing personal data, how well resourced they are, and how robust their processes are. This creates inconsistencies and different experiences for individuals when they deal with different organisations.

We welcome further guidance on complaints procedures to promote consistency and best practice for dealing with data complaints across UK organisations.

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

In the context of enforcement, we urge the government again to take account of our well-established and evidenced-based views (explained in more detail above) and implement the right for appropriate organisations representing data subjects to bring 'opt-out' collective actions. This is an essential step to ensure that there is meaningful access to justice for serious data breaches suffered by groups of individuals and greater deterrent effect of the UK GDPR on non-compliant larger companies.

If the ICO is facing difficulties in receiving the information that they require from an organisation to complete their investigation, it seems reasonable for them to be able to commission an independently produced report to inform their investigations. If an external report is to be commissioned, there should be sufficient controls in place to allow the organisation under investigation to furnish the required information. Full

2 Marylebone Road
London NW1 4DF
t 020 7770 7000
f 020 7770 7600
which.co.uk

specifications/requirements for the external report should also be shared with the organisation under investigation and any individual complainants affected.

- **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?

Which? believes that the cost of any externally commissioned report should be borne, in the first instance, by the ICO. If the investigation finds that the organisation under investigation is in breach of the law, then these costs should be reclaimed from the organisation.

- **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?

Which? supports the proposal to extend the statutory deadline from 6 months to 12 months, which will allow the ICO sufficient time to review all evidence submitted by organisations. Currently organisations have 28 days to submit their representation and the right for extension in certain circumstances, which we agree doesn't leave the ICO enough time to review often very complex evidence. This extension should not be seen by organisations as an opportunity to take longer in providing evidence to the ICO and delaying the process.

- **Q5.7.8.** To what extent do you agree with the proposal to include a 'stop-the-clock' mechanism if the requested information is not provided on time?

Which? supports the proposal for the ICO to enforce a 'stop-the-clock' mechanism to combat delays by organisations in submitting evidence required for an investigation. Organisations must also be held responsible for providing inaccurate or incomplete information that can hinder the investigation process and we are keen to see more details on this proposal.

ABOUT WHICH?

Which? is the UK's consumer champion. As an organisation we're not for profit - a powerful force for good and here to make life simpler, fairer and safer for everyone. We fund our work mainly through member subscriptions. We are not influenced by third parties – we never take advertising and we buy all the products that we test. Which? works in pursuit of its charitable objects for the public benefit.

For further information please contact Renate Samson - Principal Policy Advisor
renate.samson@which.co.uk