3rd Floor North
200 Aldersgate Street
London EC1A 4HD

Tel: 03000 231 231

citizensadvice.org.uk

19th November 2021

Citizens Advice's response to DCMS' public consultation on reforms to the UK's data protection regime.

Dear DCMS Domestic Data Protection Team,

Citizens Advice welcomes the opportunity to respond to this consultation. We are primarily responding in our capacity as the statutory consumer advocate for GB energy consumers, although some of our comments apply more generally. In this role we have conducted numerous pieces of research on people's attitudes towards sharing their data.[1] Data and digitisation, including consumer data, will be central to the transition towards a net zero energy system. It is therefore essential that people feel confident that their data is secure, that it isn't being misused, and that they can share in the value that it creates.

We recognise that the government is keen to transform its data protection framework, in order to promote a 'pro-growth' and innovation friendly regime. We understand that the current regime, in particular GDPR, is perceived by many organisations to be complicated and ambiguous. It can also be costly to ensure compliance with. Importantly, we also know that consumer data rights are often poorly understood, and that people can struggle to engage with them.[2] As such, we are in principle, supportive of reforms which simplify the current regime while improving consumer confidence and engagement. However, it is essential that any reforms aimed at simplifying GDPR do not come at the expense of consumer trust and confidence.

We agree that the UK's current data protection regime can be complicated to interpret, and compliance can create a significant burden on organisations that are processing personal data. At the same time, our research has shown that consumers have poor understanding of their data rights, and lack transparency over what data they are sharing and who has access to it. People value the ability to choose when to share their data and what happens with it. They are more likely to engage with a service if it offers this choice, even if they ultimately do not take advantage of those choices.[3] While, in principle, we support a review of the current data

[1] Citizens Advice, Clear and in Control, 2020 **&** forthcoming research into consumer protection for smart home technologies.
[2] Citizens Advice, Clear and in Control, 2020
[3] Citizens Advice, Clear and in Control, 2020

protection regime, we have a number of concerns about several of the government's specific recommendations.

We are concerned by the Government's proposal to replace the balancing test with a 'limited, exhaustive list' of legitimate interests, allowing organisations to process personal data without consent in such instances. A poorly specified or overly generic list of legitimate interests could leave the door open to misuse of personal data. Additionally, we urge the government to think carefully before implementing any of their proposed changes to the GDPR accountability framework. The existing accountability framework, although imperfect, is the main mechanism through which data protection and privacy is regulated. Any risk-based management system that replaces it should meet a high threshold for justification, and should be underpinned by clear guidance and robust monitoring and enforcement mechanisms.

When considering how to simplify the consent process and reduce 'consent-fatigue', we urge the government to think about a range of potential mechanisms, instead of removing the need for consent. We are encouraged to see that the government is considering innovative data sharing solutions as a means of collection, storing, accessing and using data in a responsible and efficient way. There are also design-based solutions that should be considered to simplify the consent process. A lot of sector-specific work is already underway to consider innovative data sharing solutions, which the government can draw upon as it considers next steps.[4]

There is a risk that proposed changes in the area of Artificial Intelligence (AI) and machine learning could lead to less transparency for consumers, and potentially worse outcomes. The proposal to remove the rights under Article 22 of GDPR 'not to be subject to a decision based solely on automated processing' where the decision has legal or significant implications, is likely to lead to more important decisions being made about people using opaque and unaccountable algorithms. We also have concerns that other proposals relating to AI have the potential to increase the misuse of personal data by organisations, with a particular risk posed to people from certain demographic groups.

The success of the UK's data protection regime, now and in the future, depends on the Information Commissioner's Office (ICO) having the right tools and resources. This includes providing effective guidance, monitoring and enforcement. It is crucial that whatever reforms are made, the ICO retains its independence. We also urge the government to consider bolder reforms to the appeals and redress process, to empower consumers to assert their own data rights.

Any changes to the UK's data protection regime should not come at the expense of EU adequacy in data relations. As the UK's main trading partner, changes to EU adequacy are likely to significantly offset any economic benefits from reforming the UK's data protection regime. It is

[4] In energy for example: the modernising energy data project, and the energy digitalisation taskforce.

essential that as the UK strikes new adequacy agreements with other countries, that consumer protections are not reduced from the level they were set at EU membership.

As discussed above, our response to this consultation comes from our perspective as the statutory consumer advocate for GB energy consumers. As such, we have only responded to the parts of this consultation that are most relevant to fulfilling that role. Below we discuss these under the relevant subheadings.

Reducing barriers to responsible innovation

The consultation notes that many stakeholders find the lawful grounds for data processing to be unclear, and that this leads to an over-reliance on the consent mechanism. The government states that this can lead to 'consent-fatigue' among consumers, and subsequently leads to lower protection as consumers are unable to assess them properly. Therefore the proposal is to create a list of "legitimate interests" for which organisations can use personal data without applying the balancing test and without "unnecessary recourse to consent".

We agree that understanding the lawful grounds for data processing can be unclear. We also agree that consumers can suffer from 'consent-fatigue'. Our research found that 37% of consumers with a smart meter cannot recall the level of consent they have provided for energy suppliers to access their smart meter data.[5] However, this does not mean that having the power to provide consent is not important to consumers. The same piece of research found that without the ability to provide consent to data sharing, the number of people who wanted a smart meter dropped by almost a third.[6]

The government should consider alternative ways for consumers to provide consent. A number of design-based solutions exist in other countries, while others have been proposed. Data trusts could act as a legal structure, entrusted by individuals to make decisions about their data use and collection on their behalf.[7] There is the potential for this to address the problem of consent being reduced to an ill-informed binary choice. In Australia, as part of their recently enacted 'consumer data right', consumers in open banking can use a portal to easily control what data they share, and change their preferences. The data right is set to be extended to other sectors, including energy.[8] We have argued for a similar concept, which could be delivered through a data dashboard.[9]

The proposal to replace the balancing test with a 'limited, exhaustive list' of legitimate interests could potentially leave the door open to misuse by organisations. This risk would be considerable, as the government notes that any list would need to be "sufficiently generic to

---

[5] Citizens Advice, Clear and in Control, 2020
[6] Citizens Advice, Clear and in Control, 2020
[7] The Open Data Trust, Data Trusts in 2020, 2020
[8] Australian Government, What is the consumer data right?, 2021
[9] Citizens Advice, The Smart Meter Data Dashboard, 2018

withstand the test of time". For example, a possible legitimate interest cited in the consultation could be for 'business innovation purposes aimed at improving services for customers'. While in principle this sounds sensible, without further clarification this could be problematic. For example, companies might argue that any purpose that increases profits will improve services for customers, as some of these savings will be passed on to them. Under this scenario, almost all business innovation activities could be deemed to be a legitimate interest, allowing companies to process personal data without consent.

On the other hand, if definitions are too specific, this could result in companies resorting to the balancing test or consent anyway. The government suggests that the list could be updated using a regulation-making power. Although this would be necessary, this could lead to an increasingly extensive and complicated list, with added confusion as interests are added or removed. Another option would be for the ICO to provide extensive guidance on the list, although this too could lead to further confusion. Crucially, sufficient monitoring and enforcement would need to be in place to ensure that organisations are using the list of legitimate interests correctly.

Any decision to remove the balancing test should only be made after careful consideration of the above issues, alongside other issues raised by stakeholders. Although the balancing test can be complicated and time-consuming to navigate, it largely provides a good level of protection for consumers. As organisations have already invested large amounts of time and resources into understanding and employing the balancing test, any changes to it should meet a high justification threshold.

Reform of the accountability framework

The accountability principle is a central principle of GDPR, which is currently underpinned by the accountability framework. The government sees the accountability framework as 'a key driver of unnecessary burdens on organisations', and proposes to replace it with a 'risk-based privacy management programme'.

While we recognise that certain features of the accountability framework currently require a significant amount of time and resources for organisations, the framework on the whole ensures that organisations handle and use personal data responsibly. Organisations have already invested large amounts of time and resources to ensure compliance with the accountability framework. Making further changes will require additional time and resources. Therefore, as with the balancing test, any changes to the accountability framework must meet a high justification threshold for inclusion.

It is important to note the specific benefits that different aspects of the accountability framework offer, in terms of data protection and privacy. DPOs, for example, offer a good mechanism for organisations to seek advice without having to speak directly to the ICO, and reflect a similar approach to risk as is present in financial services. Data Protection Impacts Assessments (DPIA's),

which the government proposes to remove, are seen by the ICO as an important tool to help organisations to 'understand and manage risk'.[10] The consultation also proposes reforming the requirement for organisations to report data breaches so that they do not need to be reported if the risk to individuals is not 'material'. While the ICO agrees that there are incidences of over reporting of low-risk breaches, they also emphasise the importance of breach reporting, both for individual cases and as insights into the wider landscape.

In theory, a risk-based management programme that reflects the data risk of a particular organisation is sensible. However, more detail on the design of the programme is required. The decision to replace the accountability framework should only take place after stakeholders have been consulted on this detail. If these changes are implemented, clear guidance from the ICO will be required to ensure that organisations are aware of their obligations, including having an accurate understanding of the level of risk that their activities pose. We agree that the ICO should be able to access an organisation's privacy management programme on request. However, the ICO will also need to have the resources and power to audit these programmes, and take action where appropriate.

If the government proceeds to replace the accountability framework with risk-based management programmes, it is crucial that consumer protections are not compromised. We recommend that the government considers the merits of the current regime, particularly as outlined by the ICO in their response to this consultation. The design of any new system should prioritise the same level of protection.

Privacy and electronic communications

The government notes that, under current legislation, 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'. The government argues that this affects the ability of organisations to 'improve their websites and services for their customers' and leads to consent-fatigue, with many consumers not engaging with the privacy information.

To address these problems the government proposes 2 options. The first option would be to permit organisations to use analytics cookies and similar technologies without user consent. They point out that in some other countries, such as France, analytic cookies are viewed as 'strictly necessary' if certain conditions are met. The second option is to allow 'organisations to store information on, or collect information from, a user's device without their consent for other limited purposes'.

As discussed above, we think that the government should explore alternative design-based solutions to address the problem of 'consent-fatigue'. Possible solutions we have discussed in the earlier section include data trusts, a consumer data right, and a data dashboard. We know

[10]Information Commissioner's Office, Response to DCMS consultation "Data: a new direction", 2021

that consumers value consent, so finding a solution that improves this process is preferential to removing the consent process entirely.

Reducing the ability for consumers to consent to analytic cookies could damage consumer trust in online tools and services. If either option 1 or 2 were adopted, clear rules and guidance would be required to ensure that organisations are applying these rules correctly. For option 1, the consultation notes that countries with similar systems, such as France, have strict conditions that must be met if consent is not required. At least as strict rules should be in place to protect consumers in the UK. For option 2 the government proposes that a 'list of exceptions would need to be kept up-to-date', meaning that exceptions would function in a similar manner to the government's proposed reform of the balancing test. The same potential problems exist as with the reform of the balancing test, where exclusions that are defined too broadly could lead to misuse of personal data.

AI and machine learning

We have serious concerns about a number of proposals in the consultation relating to AI and machine learning. We note that the government is considering how to allow organisations to use personal data more freely, for the purpose of training and testing AI responsibly. The government's proposal to remove the rights under Article 22 of GDPR is of particular concern. Article 22 protects people from solely automated decision making which produces legal effects or significantly affects them.

The government's proposal to allow solely automated decisions based on the basis of legitimate or public interests could have profound negative impacts on consumers. Although Article 22 is imperfect, having the right to human review of decisions is essential to ensure that decisions are fair, and that consumers have trust in how their data is used. Allowing automated decisions would remove these safeguards, and increase the sense that decisions are made by unaccountable algorithms. Rather than removing this safeguard, we would like the government to increase protections. This should include mechanisms that increase transparency in algorithms and consumer understanding of how decisions are made. Consumers should also have a clear route of appeal and redress if they think an automated decision is unfair. It is also critical that effective regulation is in place for AI, including powers of oversight and reporting requirements.

We are pleased to see that the government is taking the problem of bias in AI and algorithms seriously. There is a wealth of evidence that this is a problem, and it is critical that the government thinks about how to address this. However, the government's proposal, to allow organisations access to personal data without user consent for the purpose of countering bias, is not the correct mechanism to address this problem. This would very likely lead to a situation where groups with certain protected characteristics disproportionately have their data processed without their consent. There is also a risk that incorrect application of the purpose

could lead to personal data being processed for reasons beyond countering bias. Instead the government should introduce a stronger legal requirement, that requires organisations to take measures to counter bias in their algorithms. This should be underpinned by greater transparency, and increased power for the regulator to conduct audits and take enforcement action where necessary.

The government has outlined how the application of fairness, when applied to AI, is 'broad and context-specific'. It is therefore suggested that sectoral regulators may be a more appropriate 'avenue for the assessment of some aspects of fairness, especially of fair outcomes, in the context of AI systems'. In principle we agree with this proposal. In the context of energy, an essential service, concepts of fairness are likely to be different to other markets. Therefore, it makes sense for sectoral regulators to apply this concept based on their specific knowledge. However, sectoral regulators lack expertise relating to AI, machine learning and data more broadly. Therefore, the ICO should work closely with sectoral regulators to provide guidance and support when applying the fairness concept.

Innovative data sharing solutions

We are pleased that the government is interested in encouraging innovation in the way that data can be shared. We agree that data intermediaries can be a key way of ensuring that data is managed, collected, shared, accessed and used in a responsible and efficient way. As we have discussed above, data intermediaries have the potential to improve the consumer experience. As well as open banking, sectoral work in energy is underway to look at how data intermediaries can improve the consumer experience, which we have advocated for.

Data intermediaries have the potential to improve the way data works for consumers. Any data intermediaries that the government supports should prioritise solutions that increase consumer control, and transparency over data. The government should also prioritise solutions which facilitate data portability, helping consumers to transfer their data and engage with new offers.

As discussed elsewhere in our response, the government should go further and consider how innovative data solutions can improve outcomes for consumers. This includes improving the consent process, but also data portability. In Australia, as part of their recently enacted 'consumer data right', consumers in open banking can use a portal to easily control what data they share and change their preferences. The consumer data right also provides consumers with the right, and mechanism, to share data between service providers.[11]

Reform of the Information Commissioner's Office (ICO)

The success of reforms to the UK's data protection regime depend on the ICO having the correct tools and resources. This includes the ability to provide guidance to organisations on their roles

[11] Australian Government, What is the consumer data right?, 2021

and responsibilities, but also to monitor the market and carry out enforcement action where necessary. Crucially, where they have concerns over their data or over how an automated decision has been made, consumers must have a clear route to appeal and redress.

The government aims to reform the ICO's role by creating a clearer mandate for a risk-based and proactive approach to its regulatory activities. This includes 'refocusing its' statutory commitments away from handling a high volume of low-level complaints and towards addressing the most serious threats to public trust and inappropriate barriers to responsible data use'. In principle, taking a risk-based approach which focuses on the most serious threats is sensible. However, there is a risk that specific cases of consumer detriment and data misuse are not addressed.

Currently people have the right to make a claim against an organisation if they have suffered damage due to a breach of data protection law. However, the existing process is onerous and complicated. The claimant must first contact the ICO to gain an opinion on the cases. Regardless of the ICO's decision, the consumer must then take the organisation to court to compel them to pay compensation, unless they agree to pay voluntarily. The process is complicated, and the ICO recommends that consumers seek independent legal advice before going to court.

This is in contrast to the energy market, where there is a clear complaint and redress route. This includes a complaints procedure with the energy supplier, access to independent consumer advice, and an independent energy ombudsman with the power to compel suppliers to pay compensation. The government should consider a similar appeal and redress approach for data. This will be increasingly needed as more services rely on greater volumes of consumer data and more decisions are made using automatic processes. If the decision is taken to refocus the ICO towards a more high-level and risk based approach, the ICO will also need the tools and resources to launch effective investigations and take enforcement action.

We have concerns about the government's proposed changes to the ICO's accountability mechanism. In particular the proposals to allow the government a greater role in appointing the Chief Executive Officer, in setting strategic priorities, and in the development of ICO guidance and codes of practice. This could significantly limit the ICO's independence, and we urge the government to reconsider. The ICO have also raised this concern in their own consultation response.[12]

Boosting trade and reducing barriers to data flows

After leaving the EU, the government is keen to retain EU adequacy while pursuing data partnerships with other economies. This is understandable, but it is important to remember that the EU remains our closest trading partner. Any changes to the UK data regime, and

[12] Information Commissioner's Office, Response to DCMS consultation "Data: a new direction", 2021

partnerships with other countries, should not come at the expense of divergence from the EU. UK data rights should not fall below those set during European membership.

Please feel free to get in contact if you have any questions about this response.

Yours faithfully,
Tom Brooke Bullard
Senior Policy Researcher, Citizens Advice