CBI CONSULTATION RESPONSE TO DATA: A NEW DIRECTION

November 2021

Introduction

The CBI welcomes the opportunity to respond to the UK government's consultation, Data: A new direction. The CBI is the UK's leading business organisation, speaking for some 190,000 businesses of all sizes, sectors, and regions, that together employ around a third of the UK private sector workforce.

Data is a gateway to innovation. From seamless global trade to cutting edge advances in health and wellbeing, data is an essential catalyst for innovation. Though an important resource itself, determining how to use and share data is the key to unlocking its innovative potential. The UK is starting from a position of international strength in the use and regulation of data, with a thriving digital economy worth £150.6 bn, world-leading data protection standards, and a respected, independent regulator in the ICO[1]. With these assets, the UK is fostering widespread use of - and trust in - digital technologies across the economy and society. Now the UK has left the EU, it has both strong data protection foundations based on GDPR and the freedom to react quickly to rapidly changing environment.

The UK must maintain its world-leading standards in data protection, while utilising its regulatory freedom to clarify concepts, identify new opportunities for innovation and economic growth, and streamline compliance burdens. If the UK succeeds in this objective, it can create highly effective regulation fit for a dynamic, rapidly changing, data-driven world.

Data: A new direction is a timely first-step in achieving these aims. This consultation represents the government's ambitions to capitalise on the global opportunities in the digital economy and demonstrate global leadership in data protection regulation. Businesses have identified four key areas that the consultation must address to make these ambitions a reality. They are:

1) Clarify research provisions, legitimate interests, and use of AI systems to stimulate innovation and support tech adoption

a. *Create a guidance roadmap of research-related data protection provisions to reduce compliance burdens and bust barriers to innovation*

b. *Clarify the term scientific research to bolster businesses' confidence to innovate and invest*

c. *Unleash business innovation by creating a list of legitimate interests which are not subject to a balancing test*

d. *Capitalise on the opportunities in AI by allowing different sectors to develop their own guidance regarding outcome fairness on a use case basis*

e. *Article 22 is a fundamental aspect of the UK's data protection regime and data subjects' right to redress, but to improve efficacy, protect data subjects, and support business use of AI systems the Article requires enhanced clarity and guidance*

[1] DCMS Economic Estimates 2019 (https://www.gov.uk/government/statistics/dcms-economic-estimates-2019-gross-value-added/dcms-economic-estimates-2019-provisional-gross-value-added#gva-in-all-dcms-sectors) (2021)

2) Provide flexibility in the accountability framework for diverse uses of data to reduce compliance burdens

a. *Revise the UK's accountability framework to provide business with flexibility and adaptability, whilst also mitigating associated risks*

b. *Reduce the burden of Subject Access Requests by lowering the "manifestly unfounded" threshold and providing clear examples and guidance on when SARs are lawfully dismissible*

c. *Re-categorise analytical cookies to "strictly necessary" to drive innovation and produce better outcomes for people*

3) Tackle barriers to the free flow of data and maintain adequacy with key international partners to make the UK the best place to start and grow a digital business

a. *The government's proposal to change its approach to international data adequacy agreements must not risk EU-UK data adequacy*

b. *Develop business-government partnership to explore the use of alternative transfer mechanisms to drive innovation, disperse best practice across the economy, and allow the UK to showcase international leadership*

4) Reform the ICO to reflect the changing needs of a data-driven economy and maintain high data protections standards

a. *Reforming the ICO to have regards to growth, innovation, collaboration, public safety, and its international role is critical for delivering a world-leading data protection regime*

b. *Uphold the independence of the ICO to maintain business and international partner's confidence in the UK's data protection regime and ensure continued investment and innovation*

c. *Empowering the ICO to commission independent technical reports must not undermine businesses' fundamental rights and cause undue compliance burdens*

Section One: Clarify research provisions, legitimate interests, and use of AI systems to stimulate innovation and support tech adoption

Create a guidance roadmap of research-related data protection provisions to reduce compliance burdens and bust barriers to innovation

The UK champions one of the strongest data protection regimes in the world. UK data protection regulation is comprised of high standards, extensive protections for data subjects, and important restrictions for data controllers. But, to produce these conditions, data protection legislation is necessarily complex, presenting a significant compliance burden for businesses across the economy.

One area that limits business innovation is the structure of the research-related provisions that are dispersed and layered throughout the legislation. This approach creates real and perceived barriers for organisations who want to use data processing research as part of their business operations and to support their growth through innovation.

Increasing accessibility and coherence would support businesses across the economy to continue with, or start, using data for responsible research purposes. However, data protection practitioners who are experienced in and interact with the UK's data protection legislation have noted that it may not be necessary to do this via altering the legislation. This approach would inadvertently complicate the legislation for practitioners who have experience interacting with the legislation and find the structure to be logical.

Instead, government could create guidance that sits above the legislation itself. This guidance could link all the relevant research provisions and create a roadmap for those without experience or expertise in the UK's data protection legislation. This guidance would not fundamentally alter the structure of UK data protection legislation but provide a clear route to understanding and reduce the barrier to entry.

This approach simultaneously eases the compliance burden and legislative complexity for smaller businesses without the resources to grapple with the complexity of UK data protection legislation, whilst not complicating the task of data protection practitioners who have accumulated years of experience navigating the UK's data protection legislation. Guidance which creates a roadmap and links the research provisions together provides all the benefits of simplifying the legislation for the inexperienced, without hindering the UK's experienced data protection practitioners.

These alterations create the regulatory conditions for an increasingly competitive, vibrant, and dynamic digital economy that celebrates and attracts research and innovation. It reduces the barrier for entry and assists newcomers to easily explore and understand how to lawfully use data for innovative research, while ensuring that the UK's experienced data protection practitioners can continue to effectively navigate the UK's data protection legislation. This approach to improved guidance helps position the UK as a global destination for innovative research, with a world-leading regulatory regime that is accessible and empowering for both the experienced and inexperienced.

Clarify the term scientific research to bolster businesses' confidence to innovate and invest

Research and development are at the heart of business-driven innovation. In the 2020, UK tech VC investment reached a record high of $15bn, placing the UK at a respectable third in the world for investment into tech[2]. For this trend towards prosperity, growth, and innovation to continue, the government must provide businesses and investors with confidence and reassurance in their investment.

[2] Tech Nation 2021, The Future UK Tech Built, Tech Nation 2021 Report (https://technation.io/report2021/#key-statistics) (2021)

To do so, businesses support the government's proposal to create a statutory definition for "scientific research" as it relates to data processing. This provides business and other research organisations with a sound legal basis. This regulatory reassurance will bolster investor and business confidence to fund and pursue research for the benefit of the UK's digital economy.

Though businesses are happy to support adopting the definition "scientific research" from Recital 159, businesses emphasise the importance of including "privately funded" and "business research and development" into any definition of "scientific research". This approach ensures that businesses have the same levels of clarity and confidence as other research sectors and promotes businesses to continue to research and develop innovative solutions for the benefit of consumers. Furthermore, this definition signals the government's ambition to maintain the UK's high levels of private investment into its digital economy to drive societally beneficial innovation.

Simply, this legislative definition provides businesses with confidence to invest, ensuring that the UK's data regime is fundamentally pro-growth and pro-innovation. These conditions can position the UK as a global hub for investment in research and innovation.

Unleash business innovation by creating a list of legitimate interest which are not subject to a balancing test

Businesses are struggling to effectively use legitimate interests as a lawful basis to collect and process data. Furthermore, disparity between businesses' application of balancing tests is producing varied levels of protections for data subjects and uncertainty around the ICO's enforcement of the regulation. The apprehension associated with using legitimate interests has led to an overreliance on consent as the lawful ground for businesses engaging in data-processing practices, as firms try to mitigate the corresponding risks. This tendency to favour consent has a number of knock-on effects: it reduces the variety of compliance approaches utilised by UK businesses, undermines the role of consent and public trust in the research and data ecosystem, and generates undue compliance obligations.

The government is right to identify that the overreliance on consent is generating cumbersome barriers to data processing activity. However, this overreliance is also undermining the role of consent and weakening the data protection standards for data subjects. Consent is only legitimate when it can be withdrawn, and it is not the intended lawful ground for most businesses' data-related research activities. Creating a list of legitimate interests that do not require a balancing test is a useful solution to these emerging issues within the UK's data protection regime, which ensures that data subjects are sufficiently protected under the UK's data protection legislation.

To enhance the impact of such a list, businesses encourage the government and ICO to produce more extensive guidance and examples to help businesses interpret and effectively use the list of legitimate interests as the legal basis for research activities. Combining the list of legitimate interests with this improved guidance will encourage businesses to adapt their compliance operations and shift to more appropriate lawful grounds for their data processing operations.

Businesses also encourage government to seize the opportunity and take a more expansive and extensive approach to a legitimate interests list to include pro-innovation and pro-growth interests. The inclusion of bias monitoring, detection, and correction of AI systems within the list is a welcomed first step and illustrates the government's forward-thinking approach to data regulation. Businesses would welcome further clarity and guidance on the proposed legitimate interests as well as what safeguards would be necessary to maintain the high-level of protection for data subjects. The inclusion of this activity with further clarity and guidance will empower businesses and other research organisations to explore the innovative potential of AI systems as part of their operations. Government can go further and include additional pro-innovation, pro-growth, and societally beneficial processing activities in the proposed list. These could include, for example, where using personal data is an intrinsic and expected element of an innovative product or service, or for consumer impact research for a new-to-market product or service, or business intelligence on diversity, equality, and inclusion within its organisation. The proposal of a legitimate interests list is a welcomed first

step and government should explore how to best utilise the legitimate interests list as a vehicle for accelerated innovation.

It is unlikely that the list of legitimate interests will either be exhaustive in conception, nor consistently fit for purpose in a highly dynamic and innovative sector. To overcome these challenges the CBI recommends that government regularly reviews the legitimate interests list. It is important for the list and guidance to evolve over time to ensure the UK's data regime can keep pace with the digital economy and business innovation. As part of this review process, government should establish an extensive dialogue with businesses, stakeholders, and civil society organisations to identify gaps in the government's proposed list and potential new legitimate interests. These discussions will not only improve the contents of the list, but also increase awareness and encourage widespread support of the government's proposal.

This dialogue can continue into formal periodic reviews of the legitimate interests list. This will coalesce the experience, expertise, and insights of data processing organisations. Establishing new forums for dialogue on the legitimate interests list will allow the UK's data protection regulation to innovate and evolve over time. With this adaptable approach and strong foundations, the UK will continue to enrich its regime, showcase best practice, and demonstrate global leadership in data protection regulation.

Capitalise on the opportunities in AI by allowing different sectors to develop their own guidance regarding outcome fairness on a use case basis

Artificial intelligence is a transformative technology and a monumental, economic opportunity. Research from PWC estimates the total, global economic impact of AI to be over $15tr by 2030, while the CBI's Seize the Moment report argues that AI diffusion across the UK economy could add £38bn to UK GVA in the same period[3][4]. There are huge prizes for business to capture in developing and deploying AI, and there is a global race to secure these prizes. If UK businesses are to win this race, the UK's data regime must maintain its world-leading data protection standards, support trust in technology, and embrace innovation.

The proposal to develop a substantive concept of outcome fairness is an illustrative example of the government's ambition to maintain high levels of data protection and embrace emerging innovations - and businesses understand the importance of embedding fairness into technology deployment Though government is intending to unify an increasingly fragmented set of regulations that impact AI, the overarching proposal on outcome fairness threatens to create a barrier to innovation. Businesses are already using AI, from business process optimisation to virtual assistants and chatbots[5]. The impacts of AI systems on data subjects are as diverse as the use cases for business. Any substantive definition of outcome fairness would have to take this context into account, and it is unlikely that a single outcome fairness definition could effectively capture the diversity of AI use cases. This risks creating a broad definition of outcome fairness that inadvertently treats all use cases the same, regardless of their impact on data subjects, and increases complexity by layering another requirement on top of existing rules.

There are a several concepts of fairness that relate to AI systems: fair use of data, procedural fairness, and outcome fairness. Unlike the other two, outcome fairness is extrinsic to data protection. Data protection legislation ensures the fair use and fair processing of data but should not legislate for outcomes. For example, it is unnecessary to determine whether the outcome of personalised TV programme recommendations for a user are fair; what matters most within the remit of data protection legislation in this example is that the use and processing of the data to reach that outcome is fair.

[3] PWC 2017, Sizing the prize: What's the real value of AI for business and how can you capitalise? (https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf)
[4] CBI 2021, Seize the Moment. (https://www.cbi.org.uk/media/6836/seize_the_moment_report-01_06.pdf)

[5] IBM 2021, Global AI Adoption Index 2021 (https://filecache.mediaroom.com/mr5mr_ibmnews/190846/IBM%27s%20Global%20AI%20Adoption%20Index%202021_Executive-Summary.pdf)

Rather than developing an overarching, substantive concept of outcome fairness, government should encourage sector regulators to work with businesses to obtain a granular understanding of AI systems, use cases, and potential impacts on data subjects. Business would welcome guidance and case studies from regulators explaining data protection and fairness obligations as they relate to outcomes. Where fairness considerations are relevant to multiple authorities, they should collaborate to produce joint guidance that brings different regulations and laws together, thus helping businesses navigate the multiple sets of obligations identified in the consultation.

Article 22 is a fundamental aspect of the UK's data protection regime and data subjects' right to redress, but to improve efficacy, protect data subjects, and support business use of AI systems the Article requires enhanced clarity and guidance

Article 22 is an essential component of the UK's world-leading data protection standards. The Article provides data subjects with the legal right to redress should an automated decision have a legal or significantly similar effect on the individual. Businesses recognise the importance of Article 22 and the vital role of safeguards in relation to automated decision-making. However, in its current conception Article 22 is not operating as intended, and this is causing confusion for businesses and weakening the safeguards intended to protect data subjects.

Businesses recognise the fundamental importance of Article 22 and strongly support its existence within the UK's data protection legislation. However, to ensure the effectiveness of Article 22 businesses propose further clarity and guidance on the definition of legal and significantly similar effects. Human oversight is an essential vehicle for the right to redress for data subjects. However, the current understanding of the Article is holding back the expansion of AI systems and automated decision-making by inducing tokenistic human oversight on many automated decisions that do not have a material or significant impact. This approach limits innovation and prevents automated decision making from playing an effective role across society. Clarity regarding the scope of Article 22 provides businesses with confidence to use AI systems and automated decision-making more efficiently, while ensuring that data subjects have sufficient rights to redress for decisions which have a material or significant impact. These changes will position the UK as a global hub for innovation and development of AI systems, where the updated regulation supports the innovation, deployment, and expansion of AI systems and ensure high levels of protection for data subjects.

To ensure that Article 22 sufficiently safeguards data subjects and provides a right to redress, the ICO must help organisations to understand and implement best practice on appropriate Article 22 implementation. A set of case studies and questions can help guide businesses in deploying AI systems. This structured guidance will help businesses use AI systems effectively and confidently, while ensuring that the necessary safeguards are in place for data subjects. These changes will help the UK lead the global conversation in the development, deployment, and regulation of AI systems.

Section Two: Provide flexibility in the accountability framework for diverse data use to reduce compliance burdens

Revise the UK's accountability framework to provide business with flexibility and adaptability, whilst also mitigating associated risks

Government is right to explore where there are opportunities to improve the UK's data compliance regime and reduce the burden on businesses where appropriate. The UK is uniquely placed to take advantage of the strong foundations cultivated by UK GDPR and show dynamism to lead the world in improving data related regulation.

Businesses support government's ambition to lead the world in data regulation. In the years since GDPR came into force, data compliance operations have matured, and UK businesses now showcase high standards of data protection compliance. With increased public awareness of data protection, businesses now understand that privacy management is an essential aspect of business strategy and trust in technology. Due to the strong foundations of UK GDPR, data protection and compliance present an emerging market opportunity where businesses can compete with one another to distinguish themselves based on their practices and operations. Introducing Privacy Management Programmes would shift the legislation from a universal, minimum data protection threshold to a regulatory framework that encourages businesses to develop innovative approaches to data protection compliance that best suit their business model and operations.

The government is right to recognise the UK's strong foundations and investigate how a new proportionate approach to data protection can empower businesses to improve efficiency, tailor their data compliance operations, and strengthen the UK's data protection regime through a pro-competition and pro-innovation approach. If instated correctly, Privacy Management Programmes could mark a welcome first step in a more granular, sophisticated, and proportionate approach to data protection regulation in the UK which builds business and consumer trust in the UK's data protection regime. This presents a real opportunity for the UK to stand out internationally and position itself as a global leader in forward-thinking approaches to data protection regulation.

Businesses have, however, raised some concerns and potential challenges regarding the proposed changes. Businesses are concerned that removing the requirement to have Data Protection Officers may reduce the perceived importance of data protection and compliance from board and strategic level conversations within a business, while removing the necessity for Data Protection Impact Assessments could provide a false indication that data privacy and protection is taken less seriously in the UK as compared to other countries.

The consultation recognises that many of the processes currently required under UK GDPR would likely need to be incorporated into the proposed Privacy Management Programme framework. Businesses therefore require further clarity on the proposals to ensure that provisions stipulated to replace current requirements tangibly reduce compliance burdens. As such, it might be that adding flexibility to the existing UK GDPR accountability requirements would achieve the proposed benefits without involving a substantial redesign of the rules, and thus reducing the business cost of updating compliance practices across the economy.

Some businesses are also concerned that the implementation of Privacy Management Programmes may cause friction between companies who choose to embark on this new approach and those companies who retain their existing compliance programmes. The consultation is clear that pre-existing accountability frameworks will remain viable under the government's proposed changes, but businesses need further clarity and guidance on how they would be expected to manage two different compliance regimes when collaborating.

For example, two businesses are set to collaborate on a business venture requiring the use, sharing, and processing of personal data. If one business is operating a Privacy Management Programme drawn from

their legacy accountability framework and the other a newly formed Privacy Management Programme, these businesses would require further guidance as to how these frameworks interact with each other. The decision to use one framework, or the other, will create an additional compliance burden for either business or may create a barrier to innovative collaboration between business partners. Further guidance from the government and the ICO to explore a standardised approach and outcome to this challenge would be strongly supported and encouraged by businesses.

This is an example of the broader concern amongst businesses regarding the development of a two-tier or two-speed compliance regime. Businesses who operate in multiple territories are unlikely to redesign their compliance operations specifically for the UK operating territories. These businesses are thus unlikely to experience the benefit of the government's proposed changes, and this may increase regulatory friction and exacerbate their pre-existing compliance burden; especially if these changes fundamentally affect the UK's international adequacy agreements which are fundamental for businesses across the economy. This is an issue explored in more detail in the next section of this response.

Altogether, businesses welcome the government's innovative thinking and desire to update the UK's accountability frameworks. The freedom afforded by these proposals allow businesses to pursue more suitable compliance regimes that better reflect their operations and data processing activities. If government is able to provide further clarity on the proposed changes and mitigate the risks associated with legislative change, then these proposals ensure that the UK's data protection regulation reflects the diverse use of data across the economy, and empowers UK businesses to pursue efficiency, develop new best practice, and lead from the front in data protection compliance.

Reduce the burden of Subject Access Requests by lowering the "manifestly unfounded" threshold and providing clear examples and guidance on when SARs are lawfully dismissible

Businesses recognise the fundamental importance of Subject Access Requests (SARs) to demonstrate that personal data is being processed in a legal and lawful manner. SARs build trust with data subjects through establishing transparency and reinforce confidence in the UK's data protection regime as a whole. However, SARs - primarily in bulk - are costly and time-consuming.

Additionally, there is a growing trend to inappropriately utilise SARs for purposes beyond awareness and verification of the lawfulness of processing personal data. In many instances, SARs are used in employee disputes or as a pre-litigation mechanism. This – and other examples - are not the intended use of SARs and result in a notable compliance burden and cost for businesses. Some businesses are unable to deal with the workload and must partner with other firms at great expense. To prevent this growing trend, businesses support lowering the "manifestly unfounded threshold", to ensure that SARs are utilised for their proper and intended purpose; to allow a data subject to "be aware of, and verify, the lawfulness of the processing of personal data"[6].

Businesses would welcome further guidance and clarity from the ICO on what is in and out of scope under the "manifestly unfounded threshold". This will provide businesses with the confidence and reassurance to dismiss improper SARs legally and rightfully. The SARs regime should take inspiration from the Freedom of Information (FOI) regime which has much clearer exemptions and case law, which helps organisations appropriately handle requests and ensure compliance is proportionate.

By altering the regulation, government will maintain the vital role of SARs while also alleviating the concerns and undue threat they pose to businesses. This in turn, strengthens the UK data protection regime and ensures that the regulation continues to protect data subjects as well as businesses from unwarranted harm, and reinforces public and business trust in the UK's data protection regime

[6] DCMS 2021, Data: A new Direction (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf)

Re-categorise analytical cookies to "strictly necessary" to drive innovation and produce better outcomes for people

Analytical cookies are a fundamental tool for any business operating a customer-facing digital service. When used properly, cookies can produce beneficial outcomes for businesses and consumers alike. Businesses can optimise their operations and as a result consumers receive an improved service.

However, the current categorisation of strictly necessary, analytical, and tracking is causing confusion among internet users and limiting the innovative potential of cookies. This three-way separation means that analytical cookies are often grouped with tracking cookies, which are more far-reaching and do not necessarily lead to improved outcomes for consumers. Regrouping analytical cookies with strictly necessary cookies can help shift public understanding and enable businesses to make meaningful and innovative changes to the personalised services they deliver.

Businesses welcome the government proposal to remove the requirement for consent to use analytical cookies. This is an important first step in creating a more sophisticated understanding, discussion, and approach to cookies within the UK's data protection regime. Like Privacy Management Programmes, government should seek to regulate cookies within an outcome and risk-focused framework. Analytical cookies can be used for a range of essential functions, such as product development and innovation and should therefore not be subject to compliance restraints. Shifting to a more granular, proportionate, and risk-focused approach to regulation will provide consumers with enhanced clarity and transparency, while also empowering businesses to use analytical cookies to innovate and improve outcomes.

Section Three: Tackle barriers to the free flow of data and maintain adequacy with key international partners to make the UK the best place to start and grow a digital business

The government's proposal to change its approach to international data adequacy agreements must not destabilise EU-UK data adequacy

Broadly, businesses are receptive to the government's ambition to shift towards a risk-based and outcome focused approach to international adequacy agreements[7]. Data localisation and the legal complexity of data transfers present real barriers to businesses who seek growth through entering international markets. The government's shift in approach can help tackle this barrier and empower UK businesses to globally expand operations.

Businesses welcome the growing impetus government places on data flows in international trade agreements, and appreciate the example set by the UK-Japan trade deal. The government's approach to international adequacy agreements signals a clear philosophy: difference in frameworks does not have to entail divergence in standards.

Businesses agree with this sentiment but are concerned about how this shift in approach will affect the EU-UK's data adequacy agreement in practice. Businesses believe it is fundamental for adequacy to be maintained with the EU. Not only is the EU the UK's largest trade partner - making up 43% of all total exports - but it is also a critical partner for the UK's international data flows; 75% of the UK's data transfers end in EU destinations[8][9]. Prior to agreeing EU-UK data adequacy, businesses told the CBI that without a data adequacy decision, more UK companies will shift jobs abroad in data intensive areas such as HR, and increasingly invest in data centres in EU countries in place of UK ones as they see an increase in the loss of contracts with EU customers who no longer wish to deal with UK partners[10].

Losing adequacy with the EU would not only burden businesses with excess compliance obligations but threatens to undermine the positive proposals laid out in earlier chapters of the consultation. Businesses will not be able to reap the benefits of the government's proposed changes to research, nor accountability frameworks if they are forced to shift focus and resources to maintaining two divergent compliance regimes across the UK and the EU.

Businesses strongly encourage government to recognise that a world-leading data protection regime requires a framework that supports adequacy with important international partners. Such an approach will ensure that the UK continues to advance regulatory co-operation with international partners as they too assess and reform their respective data regimes. This consultation's proposals, and indeed the UK's international position are strengthened - not weakened - by mutual recognition and collaboration with like-minded international partners.

---

[7] DCMS 2021, Data: A new direction (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf)
[8] House of Common's Library 2020, Statistics on UK-EU trade (https://researchbriefings.files.parliament.uk/documents/CBP-7851/CBP-7851.pdf)
[9] TechUK 2020, Written Evidence (PBS0050) (https://committees.parliament.uk/writtenevidence/8405/default/)
[10] CBI 2020, Smoothing the cliff edge, 48 steps to mitigate disruption after the Brexit transition period (https://www.cbi.org.uk/media/6090/2020-12-smoothing-the-cliff-edge.pdf)

Develop business-government partnership to explore the use of alternative transfer mechanisms to drive innovation, disperse best practice across the economy, and allow the UK to showcase international leadership

Businesses are best positioned to determine the most effective and efficient methods of transferring data. They have a rigorous understanding of their operations, and the underpinning data transfer requirements. On this basis, it is logical to remove restrictive compliance burdens which can be unsuitable or overly-prescriptive for the type of data transfers businesses require.

Businesses would be able to pursue new and innovative approaches to the lawful transfer of data - injecting innovative approaches into the UK's data regime. Government has correctly identified that businesses cannot succeed in this endeavour alone. Though businesses are best placed to develop new approaches to data transfers based on their experience, government must play an equally important supporting role. As such, businesses generally support the accompanying proposal to formally recognise new alternative transfer mechanisms.

The combination of these proposals is the key to unlocking their full potential. Businesses are incentivised to innovate, and government can recognise these innovations to ensure that best practice is dispersed and adopted across the economy. This is an inventive approach towards future regulatory development and sets the UK apart from international counterparts. It allows the UK to react rapidly to advances in international data-transfers and uses the front-line experience of business to improve and expand the mechanisms available in the UK's data regime.

However, the benefits of this new approach are predicated on the continuation of EU-UK data adequacy. Although businesses welcome government's innovative thinking to provide more flexibility and reduce compliance burdens, these potential benefits would be negated by the extra compliance burden associated with the loss of the EU-UK data adequacy agreement. Therefore, businesses encourage government to balance their approach in this context and recognise that potential benefits may be outweighed by potential losses.

Section Four: Reform the ICO to reflect the changing needs of a data-driven economy and maintain high data protections standards

Reforming the ICO to have regards to growth, innovation, collaboration, public safety, and its international role is critical for delivering a world-leading data protection regime

As the UK's regulator for data protection and compliance, the ICO has been fundamental to the success of the UK's data regime. This success has been hard-won and achieved by the ICO's effective regulatory framework which has supported business, protected consumers, and brought benefits to the whole economy.

The government's proposals to reform the ICO are indicative of the regulator's achievements across the UK's data ecosystem. Under the regulatory support of the ICO, use of data is becoming widespread across the economy and society. The ICO now operates in a world which is incomparably different to that of years gone by, and continued success requires reform to reflect these conditions.

Businesses support the government's proposals to reform the ICO by providing the regulator secondary duties to have regard to when executing its regulatory role. These secondary duties illustrate the changing role of data in everyday life and the emerging regulatory needs of a data-driven society. Growth, innovation, competition, and collaboration represent the needs from businesses in an increasingly data rich economy. Public safety ensures that the protection of data subjects remains at the heart of any regulatory development. Finally, the ICO's international role demonstrates the truly global nature of data and the government's ambition to show leadership in an emerging regulatory field.

But government has rightly identified that the provision of secondary duties alone is not enough to ensure the ICO remains a world-leading and renowned data regulator. Government, businesses, and citizens need a framework to evaluate the success of the ICO in its growing role and across its expanded regulatory remit. Therefore, businesses welcome proposals to establish KPI's on each of these secondary duties and annual reports from the ICO.

Collectively, the proposals for secondary duties ensure the ICO is equipped to effectively regulate a mature data ecosystem, while the use of KPI's and annual reports provide transparency for society and accountability for the regulator. This new framework will ensure that the ICO builds upon its achievements and continues to be a world-leading regulator now and in the future.

Uphold the independence of the ICO to maintain business and international partners' confidence in the UK's data protection regime and ensure continued investment and innovation

Businesses have stressed the need to preserve the independence of the ICO to enable the regulator to operate outside of the UK's parliamentary cycle and avoid short-term policy objectives. Independence frees the regulator from both commercial interests and political pressure. It provides the freedom to focus on long-term stability and prosperity in regulated markets and sectors.

For international partners, this is a clear indication of the UK's commitment to the objective and impartial implementation of government policy. For investors, independent regulators provide stability to regulated markets, creating conditions of confidence to fuel investment. This confidence to invest drives innovation and productivity in these sectors over time and leads to better outcomes for consumers.

The dynamic development and evolution of the UK's digital economy is in part owed to the independence of the ICO as a regulator. To retain this position of strength and to achieve the government's ambitions of a pro-growth, pro-innovation, and world-leading data regime, the ICO must remain independent from government. Taking this into account, businesses recommend that the Secretary of State for DCMS not be given the powers to set strategic objectives for the regulator annually, and instead allow the ICO to remain

independent and focused on sustaining the long-term prosperity, productivity, and innovation of the UK's data regime and digital economy.

Empowering the ICO to commission independent technical reports must not undermine businesses' fundamental rights and cause undue compliance burdens

The proposal to introduce a new power for the ICO to be able to commission independently produced technical reports needs careful consideration, more clarity, and further consultation to ensure appropriate safeguards are provided for businesses.

Businesses require more clarification on the thresholds for triggering information requests and technical reports from firms. Though the consultation stipulates that such powers are intended to be used under limited circumstances, the proposals do not outline safeguards to prevent regular commissioning of reports by the regulator. This regulatory power adds a potentially significant burden on businesses and would undermine the wider efficiency gains made from improving the UK's data protection framework. Therefore, businesses encourage the government and ICO to provide more clarity on the thresholds and recommend that such action only occurs when a business has refused or failed to provide the necessary information by commissioning its own report and providing a copy under a limited waiver of legal privilege.

Businesses suggest any such proposal to provide the ICO with the power to commission technical reports should look at the FCA's approach to ensure firms are adequately protected. This includes the full set of protections regarding reports by skilled persons in the FCA Handbook. This proposal must also be considered in conjunction with the proposals contained in the ICO Consultation on Draft Statutory Guidance (November 2020) in which the ICO proposed to start requiring access to legally privileged information. The CBI detailed concerns with these proposals in our consultation response.

Without careful consideration and further clarity, this proposal threatens the fundamental legal rights of businesses while also creating the threat of undue compliance burdens.