Cancer Research UK submission to Department for Digital Culture, Media and Sport consultation, Data: a new direction

Introduction

Cancer Research UK (CRUK) is the largest independent funder of cancer research in the world. In 2020/21, we spent £421 million on new and ongoing research into the prevention, diagnosis and treatment of cancer. We support research into over 200 types of cancer, and our long-term investment in state-of-the-art facilities has helped to create a thriving network of research at 90 laboratories and institutions in more than 40 towns and cities across the UK supporting the work of over 4,000 scientists, doctors and nurses. The impact of our research has been transformative, with cancer survival doubling in the UK over the past 40 years. Our ambition is to see 3 in 4 people survive their cancer by 2034.

Due to the breadth of work CRUK undertakes, this consultation affects different parts of our organisation in different ways. This response details our views on those areas most relevant to our work based on our own direct experience and on what we have observed and discussed with colleagues in the sector.

We welcome the opportunity to respond to this consultation and would be happy to discuss any elements of our response further if that would be helpful.

Key points

As a research funder and an advocate for cancer patients, we have a strong interest in ensuring that research can progress unhindered: data and data-driven technologies are vital for improving cancer outcomes. We therefore support the Government's ambition to improve researchers' access to data.

However, we do not believe that there is a strong case for many of the legislative changes proposed, as better guidance and training would address many of the problems identified. We are concerned that some of the proposed changes would put the UK's data adequacy agreement with the European Union – which is vital for scientific research – at risk. There is a further risk that these proposals could damage public trust, which is essential for any improvements in data collection, use and sharing to be achieved. As has been clearly demonstrated with public and private sector scandals over recent years, public trust is hard-won and easily lost.

Chapter 1 makes proposals aimed at reducing barriers to innovation. We strongly believe that the problems identified would be better addressed through improved guidance from regulators, which must include insight into the relationship between personal data regulation and other existing UK and devolved nations laws. Alongside this must be improved education and upskilling of data users and those who are responsible for overseeing the safe use of and access to data.

In Chapter 2, we agree that the accountability framework as set out in the current legislation should be flexible, risk based and proportionate to the type and volume of data being processed. We think that the proposal for organisations to develop a privacy management programme is a sensible approach to demonstrating accountability and genuinely embedding it within an organisation.

However, we do not find the prescriptive requirements of the legislation to be overly burdensome and do not think that the suggested changes would significantly alter the way that we ensure compliance with data protection laws at CRUK.

Again, we believe that additional training and support for individuals who are tasked with implementing General Data Protection Regulation (GDPR) requirements could benefit organisations more than changing the legislation.

We do support the proposal to reduce burdens on organisations by adjusting the threshold for notifying personal data breaches to the Information Commissioner's Office (ICO) under Article 33. We believe that the current threshold often means that the process of reporting adds no real value to the data subjects affected and can inadvertently hinder an organisation's response. We do feel this is an area where legislative change could reduce the burden on organisations and on the ICO without impacting on the rights and freedoms of data subjects.

We believe that the Privacy and Electronic Communications Regulations 2003 (PECR) requires significant review. Whilst we welcome the suggestions made as part of this consultation, we believe that there is an opportunity to ensure that PECR is comprehensively updated and made fit for purpose to regulate electronic marketing and advertising, which has changed considerably since the early 2000s.

We feel that having prescriptive requirements around certain types of technology or communication methods is now unhelpful and unnecessary. We would like to see the requirements for processing personal data via electronic means brought more in line with GDPR, and organisations able to make appropriate, risk-based decisions on whether specific types of processing require consent or can rely on other conditions, such as legitimate interests.

We agree with the ambition set out in Chapter 3 to enable a scalable, flexible data adequacy regime. We believe this will be beneficial for enabling international research collaborations. However, greater clarity on the proposals is required to fully evaluate the impact of the proposed changes. Crucially, the proposed changes must avoid creating unnecessary risks to existing and future research dependant on international data transfers enabled by current arrangements.

We have no specific comments on Chapters 4 and 5 and we are supportive of the overall aim of enabling more use of personal data to improve health outcomes. However, echoing the points above, we believe that the legislation is often not the blocker and that improved education and training could be more effective. In addition, we are broadly supportive of the changes to the ICO, recognising that a strong, independent regulator is important to building public trust.

Overall, we are concerned that any changes to data protection legislation may have unintended consequences for the research sector and for other businesses. In particular, we are concerned about the impact on UK's adequacy agreement with the EU. This agreement, which will be up for review in 2025, underpins vital medical and cancer research collaborations – for instance, 32% of CRUK clinical trials involving an EU member state. It is therefore essential that this is taken into consideration before amending data protection law.

We appreciate that the Government has recognised some of the risks outlined in our response in its impact assessment, however we do not feel that this fully addresses our concerns. We would recommend that a more comprehensive and up-to-date assessment is carried out, that reflects and addresses the concerns of different sectors, before the measures are implemented.

Finally, we would emphasise the need to build and maintain public trust in data use. As such, the Government must ensure that changes to the regulations that protect public rights are communicated transparently. This is especially important around issues we know are of public concern, such as increased access for private companies and automated decision-making.

1.REDUCING BARRIERS TO RESPONSIBLE INNOVATION

As a research funder, we have a strong interest in ensuring that research can progress unhindered, which includes timely and streamlined access to data. Data, and data-driven technologies, are vital for improving outcomes for cancer patients. Difficulties and delays in accessing data can be significant. For instance, we have found that varying interpretations of the UK GDPR within and between organisations can cause confusion and delays to sharing patient data.

We therefore support the Government's ambition to improve researchers' access to data, and to provide greater clarity on the aspects of the legislation relating to research.

However, we do not believe that all of the proposals as set out are necessary to achieve these ambitions. The sector has been working with GDPR and the Data Protection Act 2018 (DPA18) for three years and a range of guidance has been developed by regulatory and other bodies. Changes risk creating confusion, affecting the UK's data adequacy agreement with the EU, and damaging public trust.

In many cases, it is CRUK's view that the barriers identified could be addressed through improved, coordinated cross-sector guidance on critical issues for researchers. These include broad consent, identification of appropriate legal basis, the use of legitimate interests, and further processing.

We would also support a greater focus on education and upskilling of data custodians, researchers and host organisations. Indeed, where a lack of confidence or knowledge poses a barrier, there is a risk that further changes to data protection legislation would cause greater confusion.

As outlined above, another significant concern is the impact that legislative changes would have on the UK's adequacy agreement with the EU. This agreement underpins vital medical and cancer research collaborations, making it easier to send patient data and test results across international borders. Joint UK-EU clinical trials, including cancer trials, rely on routine international data transfers. Some 32% of CRUK clinical trials involve an EU member state, and international trials are vital to improving outcomes from rarer diseases, such as rare and childhood cancers. Additionally, collaboration with EU member states is important for realising the potential of precision medicine, where patients with common diseases are separated into ever smaller groups based on their specific disease biology (more information on this in our response to chapter 3).

If UK data laws diverge significantly from their EU counterparts, there is a risk that the UK-EU data adequacy agreement would not be renewed in 2025 – when the agreement comes up for review. Were this to happen, it would require UK-based researchers involved in UK-EU clinical trials to arrange alternative mechanisms to share personal data with their EU-based partners. These alternative data transfer mechanisms would increase the cost of research through added complexity and legal fees, which could deter EU research studies from involving UK-based researchers and, in turn, reduce patients' access to life-saving research. **We strongly urge the Government to avoid making unnecessary legislative changes that will affect the UK's adequacy agreement with the EU.**

It is also important that the Government's proposals ensure continued access to data for organisations beyond just academic researchers. Non-profit organisations provide vital contributions using data, for instance CRUK uses and analyses various forms of data to produce cancer statistics that help to improve public understanding of cancer, inform our public-facing campaigns and advocate for particular, evidence-based interventions.

Meanwhile, for-profit organisations make a significant contribution to innovation, helping to produce treatments and drugs for the benefit of patients, which would not be possible without

secure and responsible access to data. For instance, CRUK jointly funded the development of a database of images and clinical data to improve the accuracy and efficiency of breast screening, called OPTIMAM, which is valuable for training AI algorithms. We have enabled 14 commercial organisations to get access to this data, in a controlled and legally regulated manner, which has led to the development of several products that are now being used in the clinic to reduce radiologist workloads and, potentially, to increase the accuracy of breast screening to improve patients' outcomes and experience.[1]

Finally, we would emphasise the need to build and maintain public trust in increased use of data, whether for medical research or improving public services. The Government must ensure that changes to the regulations that protect the public's fundamental rights are communicated transparently, especially around issues we know are of public concern, such as increased access for private companies and automated decision-making. CRUK also supports the British Heart Foundation's recommendation that any future reforms to reduce barriers to innovation include a public engagement plan that reaches an audience that accurately reflects the demographics of the population and that represents voices from patients and the public.

1.2 Research purposes

Consolidation of research-specific provisions

The Government's intention to help researchers navigate the relevant laws for research access is positive, but we do not think that changes to the legislative text are necessary to improve researchers' understanding and could bring negative consequences.

Accurate understanding of the legislation requires researchers and data custodians to remain abreast of derogations, evolving guidance from the ICO and to engage in horizon scanning to understand real world application, and accurately assess risk. In our view, some researchers and organisations are reliant on outdated interpretations of GDPR and the broader legal framework, which can lead them to take an unnecessarily conservative approach to sharing and reuse of data.

Consolidation of research-specific provisions within the text of GDPR risks oversimplifying and therefore adding further confusion between how data is handled in line with GDPR, and how it must be handled in line with existing statute and regulatory requirements.

It would be our preference for any confusion that exists to be addressed in guidance that consolidates and clarifies existing laws rather than by amending legislation.

Statutory definition of 'scientific research'

In this section, the Government proposes creating a statutory definition of scientific research to offer greater certainty for researchers. However, we do not believe this is a significant barrier, and **we do not agree that a separate definition of scientific research is required in GDPR**, as additional definitions would risk confusing definitions of research in existing legislation elsewhere.

[1] For instance, see: International evaluation of an AI system for breast cancer screening. Mayer, S. McKinney, Sieniek, M., Shetty, S. *Nature* volume 577 (2020) www.nature.com/articles/s41586-019-1799-6

In our experience, most, if not all, researchers, are aware that their research is considered scientific research, and they tend to think proactively and expansively about data. Reassurance in this area is more likely to be useful for legal and governance teams in host institutions, who will often be involved in determining the most appropriate regulatory pathway to access data – but we would emphasise that we do not believe a statutory definition is required.

Should Government decide to include such a definition, that set out in Recital 159 could be a valid basis, but additional guidance on how this would be specified outside legislation – which is where it is usually used by research and funder regulatory bodies – would be needed. We would also note that, given that cutting edge science pushes boundaries, any definition would need to be very carefully considered to ensure it stands the test of time. **We would urge the Government to ensure that the research community is consulted before any definition of scientific research is finalised**.

Lawful grounds for personal data processing for research

We do not believe that identifying a lawful ground for personal data processing is a significant barrier for research. Although we have seen issues arise as a result of simplistic and outdated readings of GDPR and the DPA18, we do not believe these are because of difficulties identifying a lawful ground.

Moreover, there is already guidance from the Health Research Authority, the Medical Research Council and the ICO that university research projects can rely on tasks in the public interest as a lawful ground. This suggests the problem is a lack of awareness or use of existing guidance, not an issue of legislation.

Similarly, we strongly disagree with the suggestion to create a new, separate lawful ground for research. This will not address the root cause of the problem and could lead to further confusion. There is also a concern that, by effectively lowering the bar for processing data for research purposes, such a change may have a negative impact on public trust.

We feel it is unnecessary to change legislation and would prefer to see efforts to increase awareness of existing guidance and ensure that the existing, suitable lawful grounds are used.

In addition, we are concerned that further divergence from the main body of GDPR is not in the best interests of researchers or data subjects. It is vital that research across borders is as frictionless as possible**. The UK should not seek to add lawful bases to the body of legislation that may not be applicable for projects that require cross-border collaboration with other EU states**.

Broad consent

We agree that the issue of consent can be limiting in some situations, and that there can be some confusion around the difference between consent to participate in research and consent for personal data processing. However, **we do not believe a change to legislation is necessary; again, improved guidance will better address this problem. We would also urge Government to ensure that any changes to consent do not undermine its meaning.**

We would note that much health and medical research does not rely on broad consent. The consent to participate in research from the outset must make clear the reuse potential and further purposes, and participants should be given the opportunity to consent at that point. The legal basis for the

broader elements of the work would then likely fall to public task or legitimate interests. Any newly identified purposes would then either be related to the original research or a brand new purpose in line with ethical and other research governance standards. As such, changing legislation is not likely to affect what research can take place.

Neither do we think that bringing existing advice into the main body of the text will have any practical use, as, in our experience, few researchers are familiar with the legislative text.

However, clarification that the consents for participation that are gathered initially are valid would be a useful tool in encouraging researchers to consider secondary use at the point of gathering initial consents, and help to make this the default position.

The Government also proposes 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 where it would require a disproportionate effort to do so.

We are concerned about the potential for this to result in data controllers reverting to a default position that informing the data subject is disproportionate in all cases, due to the cost and efforts required to inform large numbers of data subjects for proposed secondary use. We agree that such risks should be assessed and mitigated, with a requirement for robust assessments where this exemption is relied upon.

1.3 Further processing

This section of the consultation sets out a series of proposals to alter the UK GDPR with clarifications around further processing, including: the conditions under which further processing may be lawful; when further processing can be undertaken by a controller different from the original controller; the distinction between further processing and new processing; and when further processing may occur, when the original lawful ground was consent.

Again, we do not see any benefits to altering the legislative text and there is a risk that changes would only bring further confusion. **We would recommend that, rather than changes to legislation, there is a greater focus on improving the understanding and application of existing guidance.**

It is true that performing an accurate assessment of the compatibility of purpose for reuse requires understanding of the nuances of the legislation, and that not all research groups or host institutions hold this level of understanding. But this is not something that should be addressed by amending the legislation. Similarly, clarification on when further processing can be undertaken by a controller that is different from the original controller should be made in sector-by-sector guidance.

From a research perspective, any clarification of the distinction between further processing and new processing should clearly define the processing relationships where a purpose may include additional research related to a disease area or broader hypothesis that requires additional data processing, or where a brand new research question that bears no relationship to the original data collection research would be a case of new processing. This should be included in guidance.

We do believe that there needs to be better guidance around when further processing may occur when the original ground was consent – although, as mentioned, in a research context, consent will rarely be the legal basis for data processing originally. Reference needs to be made against where consent was sought and either an amendment to that consent will need to be sought, or the data

will need to be rendered anonymous, or indeed statutory exemptions may apply. We believe it is important that this process is clarified.

1.4 Legitimate interests

The Government suggests that uncertainty around which lawful basis to use may have resulted in an over-reliance on consent. As outlined above, consent is rarely used as the lawful basis for research; those who access or use health data in the UK tend to use public task or legitimate interests.

However, CRUK also processes personal data to support other aspects of our work, and we do recognise that there are some circumstances where there is a tendency for controllers to be over-reliant on consent. It is possible this is driven by public perception, sometimes supported by the ICO and other privacy bodies, that consent is the gold standard. An organisation may then feel the need to justify why they are not relying on consent, which can be especially problematic in the charity sector, which is very reliant on public trust.

We do not believe this is a problem that would, or needs to, be solved through legislative changes. Further emphasis from Government and the ICO on the fact that the other conditions are equally valid would assist organisations to be more confident in relying on the legitimate interests condition for a broader range of processing.

The Government suggests the creation of a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test, which it suggests may discourage unnecessary use of consent.

We note that doing an assessment as detailed as that suggested as best practice by the ICO is not a requirement of GDPR. We feel it would be helpful to set out the circumstances where purely documenting that the processing is reliant on the legitimate interests condition (for example as part of the Record of Processing) and being able to provide a justification if required would be sufficient to meet the accountability principles. We expect this could cover situations where the processing is necessary and expected as a result of an action taken by a data subject. For instance, as a charity we rely on the legitimate interests condition to process a supporter's personal data when they make a donation.

Were such a list to be implemented, it would need to be clear that the specific processing does still need to be necessary for the purpose, and that the business would need to carry out this part of the three stage legitimate interests assessment. In addition, they would need to consider how they would ensure that they can enable objections to processing if these are received.

We do not believe that a list would in practice significantly reduce burdens, and we disagree with this proposal for the following reasons:

We are concerned that such a list would become out of date and need updating relatively frequently

The creation of such a list is unlikely to be beneficial to data subjects; lessening requirements for a balancing test is rarely likely to impact subject rights positively

Many of the items proposed could be handled with alternative bases than legitimate interests or consent - for instance safeguarding (point a in the proposed list) and network security review (point e in the proposed list)

Meanwhile, some of the activities listed that we believe would fall under legitimate interests are ones that we believe are most in need of a balancing test, and therefore should not be exempt. For instance, items related to audience measurement cookies (point d) and on use of personal data for internal research and development (point h)

We are concerned a list may create over-reliance on legitimate interests or reduce the consideration data controllers give to the rights and freedoms of the data subjects

Should this approach be taken forward, we would want to see the balancing test maintained for children's data, irrespective of whether data is processed for a listed activity, both to ensure protection from an inherently vulnerable group and because any move to reduce protections for children may risk the UK's adequacy status in the long term. We note, though, that this would create different requirements for data processing that could include both children and adults, for instance audience measurement cookies, and it is not clear how this issue would be resolved. We believe this will be just one example of situations that would need to be fully considered and addressed before a list of legitimate interests could be implemented.

We do appreciate that for some organisations, carrying out a legitimate interests assessment can be difficult. In our experience, the ICO's legitimate interests assessment guidance and template are both comprehensive and helpful for assessing processing that is more likely to be privacy intrusive. As a result, however, it is quite long and likely to be overwhelming for non-specialists.

It may be more effective in the long term to provide example legitimate interests assessments for standard types of processing, including, but not limited to, the kind of processing the government is proposing to exempt from undertaking the balancing test. This would help organisations to make consistent decisions, informed by a broader consideration of the potential impact of processing that the Government could provide – but crucially without removing the requirement to ensure that the processing is necessary in their specific situation.

In our own experience of upskilling non-specialist colleagues, we find that once they have seen a worked example they are better able to understand what the questions are really trying to get them to think about in relation to their own processing. Over time, therefore, we feel that this will also help organisations to feel more confident when undertaking less straight forward assessments.

1.5 AI and Machine Learning

There is currently a lack of clear legislation around development and deployment of AI systems, and therefore too little control or oversight of this technology. The Government identifies fairness as an area that requires clear legislation, an assessment we agree with – but fairness in AI is not specifically or exclusively a data protection issue.

As such, we are not convinced that this should be part of data protection legislation. Rather, we would support this being included in separate, AI-specific legislation, which we believe should be introduced and read alongside the GDPR.

We would also recommend that, in the absence of legislation and associated guidance, the Government does not, as proposed, permit organisations to use personal data more freely to train and test AI systems, as there would be no basis to define appropriate safeguards.

The Government is right to recognise the importance of addressing and seeking to eliminate bias in AI systems, which is essential to ensure that they do not exacerbate existing inequalities, including

health inequalities. This is a significant concern, and we are glad it is being considered. We agree that there would be a benefit in greater clarity on how sensitive personal data can be lawfully processed for the purpose of ensuring bias monitoring, detection and correction in relation to AI systems. Again, we feel that the most appropriate place for this would be in a new AI-specific legislative framework or guidance; inclusion in Schedule 1 of DPA2018 is unlikely to provide the necessary clarity.

In terms of regulation, it is likely that the ICO would have an overarching supervisory authority role from a data protection perspective, but clear boundaries need to be set for when its role overlaps with other appropriate authorities, for instance regulators overseeing development of medical devices and health intervention products.

Finally, we strongly disagree with the proposal to remove Article 22 of UK GDPR – as outlined earlier in this submission, divergence from the GDPR on key issues that protect the rights and freedoms of data subjects risks a situation where the UK loses its adequacy status, and subsequent negative effects on research. **We strongly recommend that the Government does not proceed with the proposal to remove Article 22 of UK GDPR.**

1.6 Data minimisation and anonymisation

In this section, the Government asks whether it is necessary to clarify the test for when data is anonymous by giving effect to the test in legislation, and whether the text should confirm that the re-identification test under the general anonymisation test is a "relative one". In common with our other comments in this section, we do not believe changes to the legislation are necessary. Again, we believe the issue would be better addressed through improved guidance, which is more flexible and easier and quicker to update than legislation.

We believe that the forthcoming guidance from the ICO on anonymisation, pseudonymisation and privacy enhancing technologies will be welcome and helpful, and do not believe that at this time any further legislative reform is required. Given the speed at which this area develops and evolves, we would be wary of a legislative requirement favouring a particular approach or becoming obsolete relatively quickly.

Trusted Research Environments

Trusted Research Environments (TREs) provide a secure space for researchers to access and analyse data without that data leaving that environment where the researcher goes to the data within a capable analytics environment as opposed to the data going to the researcher. CRUK strongly supports the use and development of TREs, and we have been working with the TRE paradigm internally for our analyst teams for some time. We have also established a TRE to support our funded researchers and other academic, public and third sector partners who work with us in the fight against cancer.

We envisage our TRE as a means of adhering to not only the Five Safes[2], but enhancing these with trustworthy, independent and external certifications through the ISO 27000 series and Data Security

[2] Safe people; Safe projects; Safe settings; Safe outputs; Safe data. For more information, see: https://blog.ons.gov.uk/2017/01/27/the-five-safes-data-privacy-at-ons/

and Protection Toolkit amongst others by working with fully certified Cloud Service Infrastructure Providers.

It is essential that, as numerous TREs are developed by different organisations, close attention is paid to ensuring that they are able to work together, and that both NHS and non-NHS data can be linked. Equally important are the creation of common standards and certification for TREs. CRUK strongly believes that these standards should be developed collaboratively across the sector, and that an independent body will need to certify TREs and audit against these cross-sector standards. As with all discussions about data use, meaningful public and patient involvement must form a fundamental part of TRE development.

It is important to note that anonymity is often virtually impossible to achieve for health data, and we should be vigilant to the risk of re-identification. Furthermore, cancer research often requires some degree of linkage, and so completely anonymous data would not properly benefit researchers or patients. Working within a TRE would provide the necessary security required when working with data that may be identifiable, but would still require compliance with GDPR.

We see the TRE paradigm as one that assures GDPR and other regulatory compliance by providing a safe environment for our researchers to work within. In addition, it ensures that the complexities of regulatory compliance are handled by our expert teams, rather than leaving it to our researchers to have to navigate without support or where their focus must be on conducting the research.

This is another tool in the arsenal of demonstrating trustworthy uses and protections of data and **we would welcome clearer guidance on the interpretation of those regulatory needs**, perhaps drawing on the experience of setting up TREs and the required processes. This does not require legislative change, especially that which would add further confusion to the already complex data protection and research governance regulatory space. We would propose that TREs within research and across sectors be seen as mechanisms to adhere to regulation and alleviate the uncertainty that it can cause.

2. REDUCING BURDENS ON BUSINESSES AND DELIVER BETTER OUTCOMES FOR PEOPLE

2.2 Reform of the Accountability Framework

CRUK is a large charity that processes a substantial amount of personal data relating to supporters, advocates, staff and researchers. We believe that the responsible use of personal data should be at the heart of everything we do. We invested in an organisation wide change programme in preparation for GDPR and have a permanent data protection team, who, alongside legal and information security teams, maintain a Privacy Management Framework similar to that proposed by the Government.

We agree that the accountability framework as set out in the current legislation should be flexible, risk based and proportionate to the type and volume of data being processed. We think that the proposal for organisations to develop a privacy management programme is a sensible approach to demonstrating accountability and genuinely embedding it within an organisation.

However, we do not find the prescriptive requirements of the legislation to be particularly or unnecessarily burdensome and do not think that the suggested changes would significantly alter the way that we ensure compliance with data protection laws at CRUK.

We also recognise that there needs to be a certain level of consistency in terms of how organisations interpret and comply with the framework, which becomes harder to achieve the more the framework moves away from being prescriptive. From working with our own internal teams and speaking to other charities who don't have dedicated resource, we know that often non-specialists find it easier to comply with requirements that are prescriptive because they do not have the knowledge and confidence to take genuinely risk based decisions. There is a danger that many organisations, especially in the charity sector, which is relatively risk adverse, will err on the side of 'best practice' requirements even where this isn't necessary or proportionate in their circumstances. Some examples of this are discussed in the individual sections below.

Overall, whilst recognising a benefit from some of the proposed changes, our concern is that in practice these changes are unlikely to significantly reduce the burden on business, and that understanding and implementing these changes, so soon after implementing GDPR and the impact of leaving the EU on international transfers, will add burden.

We believe that additional training and support for individuals who are tasked with implementing GDPR requirements could benefit organisations more than changing the legislation. We therefore recommend that DCMS considers how this may be achieved alongside any proposed changes that are taken forward.

It needs to be recognised that effective data protection requires individuals who are skilled at understanding data flows, risk management and the impact on data subjects. Expecting non specialists to implement these requirements is often why they feel burdensome to organisations.

Data Protection Officer

At CRUK we are required to have a data protection officer (DPO) and we decided to subsume this role under our existing role responsible for data protection compliance across the organisation. For us, it was not difficult to appoint a suitably independent DPO.

We believe that having a well understood and consistent role within organisations that process significant amounts of personal data is beneficial to organisations and to data subjects.

The tasks defined in Article 39 are reasonable for all organisations to have a nominated and qualified individual carry out. We also feel that the requirement that the person holding the role should be allowed to carry out their role without interference and report their views to senior manager directly is beneficial to ensuring that the role is carried out in an independent way. However, we recognise that there are some practical issues related to correctly identifying whether an organisation needs one, and, if so who it should be.

The guidance and definitions around what constitutes 'large scale processing' and 'systematic monitoring' are currently quite circular and unhelpful. Organisations are advised to take into account the 'number of data subjects' and 'volume of data', but are not provided with any absolute numbers, which would help consistency. Therefore, one organisation may define 'large scale' as relating to a thousand data subjects and another a million. Given that organisations who do not appoint a DPO if they should have done may be fined, we find it likely that many organisations err on the side of caution rather than make a decision that the regulator later decides was incorrect.

We, and many organisations we spoke to, also struggled in our analysis to identify exactly how 'independent' the DPO needed to be, partly because at the time there was no guidance on this, and there remains no UK based case law on this point to assist business to make an informed decision.

The requirement that the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data is overly restrictive. Very few senior level roles in an organisation make no determination at all about the purpose and means of processing, even if this is not a focus of their role. However few organisations, especially small and medium-sized enterprises (SMEs), can justify a senior, standalone role focused on data protection compliance.

We note that since 2018, an industry of external DPOs has become established, providing this service to organisations that feel there is no one internally who is sufficiently independent to take on the role.

The risk of this model is that the DPO is then viewed as semi-regulatory, rather than part of the organisation and therefore not able to influence business teams in the most effective way. We believe that our internal DPO has been able to successfully embed concepts like Privacy by Design in large part because they are seen as a trusted colleague who understands the business needs.

An effective, qualified DPO should be able to consider the legality of processing in the round and make decisions about processing even where they might also determine the purpose and means of the processing activity. Whilst we understand the need for the DPO to be able to question and hold to account senior business stakeholders, we don't feel that the role being strictly independent is necessary.

We note that the proposal to mandate a privacy management programme includes the designation of one or more 'responsible individuals' to oversee the programme and monitoring compliance, effectively taking on the requirements currently carried out by the DPO.

We feel that there is value in continuing with the DPO as a recognised title, as this has helped to add a level of structure and consistency to the profession. We would also advocate for increased training, qualifications and professional standards to ensure that businesses are properly supported to implement GDPR in a pragmatic and cost effective way.

If not mandated, we will continue to have our DPO carry out the tasks defined in Article 39 and report regularly to senior management on our compliance with GDPR. We believe it is likely that other organisations that already have an internal role will do similar, but that organisations who have outsourced the role will cease to do so.

Finally, although we are not directly affected by the proposal to remove the requirement for all public authorities to appoint a DPO, we are concerned at the impact this could have on data subjects and on public perception. Public sector organisations hold and have access to a significant amount of personal data, often linked to sensitive services. In addition, there are more, and more complex, legal bases on which public sectors bodies can rely. **We recommend that if this proposal is pursued, it is on an exception basis, with a public body required to demonstrate that they process very little or very low risk personal data.**

Data Protection Impact Assessments

We disagree with the proposal to remove the requirement to undertake a data protection impact assessment (DPIA) in the particular circumstances currently mandated. We believe the removal is unnecessary and will reduce public trust in organisations that undertake high risk processing, especially with regard to health data.

Privacy by Design and Default is a key element of data protection law. It drives compliance and ensures that systems, tools and processes are implemented in a way which reduces risks to data subjects as much as possible. As an organisation, CRUK has put in place processes which ensure that for all planned new and changed data processing we capture enough information to:

- Capture the information required by Article 30 (records of processing)
- Describe the flow of data including what systems will be used to process it
- Ensure that fair processing requirements are met and that a legal basis of processing has been determined
- Ensure appropriate security controls are in place
- Identify whether additional assessment is required; e.g. a DPIA, more detailed Legitimate interests Assessment or supplier due diligence.

The requirement to carry out a DPIA is therefore helpful in both principle and practice as it forces organisations to review and document the risks associated with their processing. Over time we have amended our DPIA template from that provided by the ICO, and created templates for specific types of processing, such as employee monitoring, to better meet the needs of our organisation and our stakeholders.

As business teams have come to better understand the rationale for DPIAs, we have been able to suggest changes at system design stage which not only improve privacy, but also ensure better user experience, reduce data storage and limit costs. We believe that effectively integrating DPIAs with other information risk and quality management systems can drive real value for organisations.

We also note that consistency of approach is very helpful in supporting cross organisation working. Where partner organisations or suppliers need to provide evidence that they have effective controls in place, providing a completed DPIA can give data controllers confidence and reduce the requirement for them to then do their own risk assessment.

We note that the requirements for carrying out a DPIA set out in Article 35 are relatively high level. We believe that the current legal framework allows more flexibility than is perhaps apparent from the ICO guidance and template. We are unable to identify an alternative risk assessment tool which

minimise data protection risks whilst not in some way providing the information which is set out in Article 35.

We do recognise that full DPIAs are difficult to complete without specialist knowledge and this is an obstacle. **We therefore strongly advocate for increased guidance and training in the use and completion of DPIAs.**

The consultation states that risk assessment tools must still be used. We welcome the opportunity for flexibility, but it is not clear from the consultation what would be required in terms of the level of detail and input required for such risk assessments. **We recommend DCMS clarifies its proposed alternative to DPIA.**

We are concerned that taking away the requirement for DPIAs may potentially create uncertainty as to how and when risk assessments should be carried out and how detailed they need to be. This is something that would need to be clarified through detailed guidance.

Article 30 Record Keeping Requirements

CRUK believes record-keeping is crucial from a compliance perspective and that as an organisation we have developed a good approach under the existing UK GDPR requirements. On that basis, we would not support the proposal to remove record-keeping.

Article 30 requires an organisation to collate information on the purposes of the processing, the categories of the data subjects, the organisations with whom the data has been shared, and (where possible) how long the data will be kept for and what security measures are in place.

We note that the proposed Privacy Management programme would include the requirement to hold Personal data inventories which describe and explain what data is held, where it is held, why it has been collected and how sensitive it is.

Both of these set out information which is useful for an organisation to hold in order to properly manage privacy risk, with considerable overlap in practice.

Since the initial data gathering exercise ahead of GDPR we have built on our Record of Processing and it now holds additional information. For example, the source of the data, the Legal Basis of Processing, the owner of the processing activity, links to systems and suppliers, the volume of data, and its inherent risk level.

It is the foundation of our approach to Privacy by Design and the way that we engage with colleagues about their activity. We are able to link the record to any assessments we have undertaken and maintain a record of decisions we have made.

Article 30 provides a reasonable basis for even small organisations to understand their data processing, and therefore a level playing field for organisations. There may be some attributes listed that are less useful than those we chose to collect ourselves, but all of those included in Article 30 are useful and organisations are free currently to collect anything else they deem useful.

Whilst some of the information we collect in the Records of Processing is also then provided to the public in order to meet Article 13 and 14 requirements, we do not believe that this is problematic. The information required by Article 30 has a much broader purpose and therefore is likely to be at a more detailed level. For example, we would have several entries in our records of processing for various elements or types of ‘fundraising’ where this is done by different teams or using different

systems, but would only speak about 'fundraising' in general terms in our Privacy Statement. We do not believe that they are interchangeable in the way suggested within the consultation.

Although we can see some longer term benefit for replacing Article 30 with a broader, less prescriptive requirement to hold a personal data inventory, we would strongly recommend that it is not removed in the absence of that alternative.

Data Breach Reporting

We support the proposal to reduce burdens on organisations by adjusting the threshold for notifying personal data breaches to the ICO under Article 33. We believe that the current threshold often means that the process of reporting adds no real value to the data subjects affected and can inadvertently hinder an organisation's response. We believe that improvements can be made in this area irrespective of whether the privacy management programme is introduced.

The requirement to report a breach 'unless the personal data breach is unlikely to result in a *risk* to the rights and freedoms of natural persons' is an unnecessarily low benchmark when considering that any breach of confidentiality is some magnitude of risk to the individual impacted. We believe that this is why organisations report almost all breaches, especially given the additional penalties for not doing so.

A requirement to report a breach 'unless the risk to the individuals is not material' is still subject to interpretation and would need very clear guidance. In addition, the negative language in which these thresholds are expressed is confusing even for experienced data protection specialists. **We recommend changing the threshold to 'organisations must report a breach where there is a material risk to individuals'.**

However, we do not think that the suggested replacement threshold will entirely negate the problems experienced for the following reasons.

The bar to report a breach to the ICO is lower than reporting to the data subject. In this way we feel that the legislation is too focused on the potential for the regulator to sanction the organisation and not enough on the requirement for the organisation to contain the impact of the breach, including for example enabling the data subject to take action to prevent any material impact, for instance identity theft.

Small breaches that have a material but relatively low risk to data subjects happen frequently (such as paper forms getting lost in the post, a letter being sent to the wrong individual, or access controls being incorrectly applied and a document being accessible to people who shouldn't see it). Organisations should and do manage breaches of this kind by assessing what went wrong and ensuring that additional controls are put in place.

We also feel that the requirement to report within 72 hours, except in the most serious of breaches, is unnecessarily short. Trying to assess whether the breach should be reported or not is a distraction for teams at the point at which they should be focusing on containing the breach and speaking to the individuals affected, if necessary. This is compounded in the charity sector, as we will also need to consider whether to also report the breach to the Charity Commission as a 'serious incident'. The ICO does not assist organisations to contain their breaches, so the reporting period could be extended to, for instance, 7-10 days without impacting on the protection of data subjects.

We believe that it would be a more effective use of the ICO's resources if it could focus on investigating breaches that have a material impact on a significant number of data subjects and/or create a high risk for a few data subjects (e.g. where special category data is involved). This is in line with the ICO's own regulatory action plan, suggesting that many breaches are reported and closed without meaningful input from the ICO already. Our view is that this does not benefit data subjects, while at the same time increasing the burden on both the regulator and the organisation.

In relation to the proposed voluntary undertakings process, we are unclear how this would differ materially from the current process. Under the current regime, an organisation will normally report both that an incident had occurred and the plan of action they propose to take. Given the number of breaches which are reported, and the level of published enforcement action taken by the ICO, we can only assume that quite often it accepts this plan and takes no further action. We would appreciate more clarity on this proposal.

2.3. Subject Access Requests

As an organisation, we receive very few subject access requests from supporters or researchers. Most requests we do receive are from members of staff or volunteers, and tend therefore to be quite complex and involve reviewing a lot of information to identify what is actually personal data. These can take up the full time of members of the team dealing with requests, to the point that other work is de-prioritised to ensure deadlines of the requests are met.

The issues which generate or elevate costs include:

- Unstructured data. Unlike data held in Customer Relationship Management systems, information relating to staff and volunteers is often included in emails, photos, CCTV and documents. Often these are primarily business related, and therefore significant time is taken identifying information that relates to the individual in a personal capacity. They may be held by a number of people across the organisation, and knowledge of context is important in identifying whether or not something constitutes personal data.
- Data subject expectations around what is recorded. Sometimes data subjects receive less than they thought they would, either because formal records of an issue were not created or something they think happened or was said wasn't. It can be difficult to prove a negative in these circumstances. Documents that have been heavily redacted because the bulk of the content does not relate to the individual can also make data subjects suspicious.
- The requirement to provide the data subject with additional information about the data we hold. For example, where we got the information from, international transfer safeguards, reasons for holding data, even where they have not requested this and are not interested in it themselves.

We very rarely receive repeated requests, and where we do this is usually because of an ongoing issue, and so new information is held.

Our view is that the level for subject access requests being assessed as manifestly unfounded is acceptable. The guidelines give quite clear examples of what could be viewed as manifestly unfounded and it is for each organisation to assess their own requests. We note that often requests do come as a way to try and understand or resolve a situation which has caused the data subject distress or concern, and – whether unfounded or not – negative feelings about the organisation may be communicated as part of the request for their data in a way that could be interpreted as

malicious intent. We would be concerned that if the threshold is lowered, data subjects could be excluded unnecessarily from accessing their personal data.

As an organisation we chose not to charge a fee to access information under the Data Protection Act 1998. Although we do recognise that a small barrier to stop people putting in speculative requests is helpful for organisations that receive significant numbers of requests, we do not believe that it would be appropriate for us to restrict access to data based on an ability to pay.

One area that we do believe could reduce costs is to introduce a requirement for requesters to narrow down the scope of their request and/or confirm the nature of their relationship with the organisation. If used alongside a requirement for the organisation to assist, similar to that found under Freedom of Information, we believe that this may better ensure that the data subjects receive the information they require whilst limiting the burden on organisations. **We recommend Government considers introducing such a requirement.**

In addition, we would support better guidance for data subjects on what constitutes personal data, especially in situations where they have a professional and personal relationship with an organisation.

2.4 Privacy and electronic communications

We believe that the Privacy and Electronic Communications Regulations 2003 (PECR) requires significant review. Whilst we welcome the suggestions made as part of this consultation, we believe that there is an opportunity to ensure that PECR is updated and made fit for purpose to regulate electronic marketing and advertising, which has changed considerably since the early 2000s.

Overall, we feel that having some very prescriptive requirements around certain types of technology or communication methods is now unhelpful and unnecessary. We would like to see the requirements for processing personal data via electronic means brought more in line with GDPR, and organisations able to make appropriate, risk based decisions on whether particular processing requires consent or can rely on other conditions, such as legitimate interests.

Confidentiality of terminal equipment, including the use of cookies and similar technologies

As noted in the consultation, the requirements in Regulation 6 are not risk based, are burdensome for organisations and lead to data subjects 'consenting' without taking the time to understand what they are consenting to.

Whilst the regulation and guidance do reference 'similar technology' there is a lack of understanding about how these technologies differ from cookies, and how much more 'real life' personal data some tracking technologies make use of. **We would welcome additional guidance on understanding risks of these emerging technologies.**

We agree with the proposal that organisations should be able to use analytics cookies and similar technology without the user's consent. We recognise that if any other type of personal data were processed for this purpose, it is likely that an organisation would be able to demonstrate that the legitimate interests condition could be relied upon.

We also believe that requirements for information captured for the purpose of analytics to be aggregated and pseudonymised already provides a level of protection to people visiting websites.

At the moment, analytics is only used to cover onsite analytics (i.e. information gathered by 1st party cookies). We believe that the purpose of analytics should be expanded to include collecting conversion data back to publishers. It should be accepted for a company to be able to send conversion data back to advertising network, to be able to attribute channel performance and optimise marketing. This is because the technology for measurement and targeting on ad networks is linked. Under the current framework we need to decouple the targeting from the measurement aspect of a marketing pixel to enable analytics without necessarily allowing the targeting.

We would also advocate for a risk based approach to be taken for other kinds of cookies, including those often classified as performance cookies, which while not strictly necessary do significantly improve the experience of using the website whilst not impacting on individuals privacy in a meaningful way.

If PECR's requirements for consent for all cookies were removed, organisations would still need to comply with the principles on lawfulness, fairness and transparency under GDPR. Due to the nature of the real time bidding and broader online advertising ecosystem, it is likely that some tracking technology will still require consent. The difference will be that this is based on an assessment of that particular processing activity. It would likely be appropriate that a DPIA be carried out, and we would support the development of sectoral codes or further regulatory guidance to enable organisations to carry these out in a consistent way.

We are concerned by the proposal that consent for such technology be set by browser, software applications or device settings. The risk is that people take a blanket approach to cookie consent across all websites.

Currently, people can make their choice based on their feelings and trust towards a specific brand. For example, more than 95% of our website users choose to consent, and we think that this would be significantly reduced if consent was set at a browser level. We do not believe that this would necessarily combat the issue of consent fatigue.

Another risk is that we would be unable to tailor the wording at browser level. We have already seen a negative impact from that lack of input in the IOS changes, where Apple requested consent using wording that placed a bias on opting out. It does not seem fair to allow browsers (with their own conflicting priorities) to control website permissions.

We recommend that consent for cookies and similar technologies is not set at browser level.

If we were to make opt-in at browser level (or another solution that is different to cookie opt in banners) it would be less of an issue to us if the analytics point about extending out the definition of analytics is implemented. This would mean the only requirement for consent would be for pixel retargeting/lookalike modelling via walled gardens (like Facebook and Google with login capability) since we are losing third party cookies anyway which enable retargeting outside of walled gardens.

The soft opt in

We believe that the way the soft opt in was drafted is unintentionally restrictive and unnecessarily differentiates between marketing of products and services and direct marketing about other things.

This element of data protection law is the only place where the definition of 'direct marketing' is restricted in this way. The ICO define it normally as follows:

> Direct marketing is not limited to advertising goods or services for sale. It also includes promoting an organisation's aims and ideals. This means that the direct marketing rules in the Data Protection Act (DPA) and PECR will apply to the promotional, campaigning and fundraising activities of not-for-profit organisations. For example, a charity or political party contacting particular individuals to appeal for funds or votes or contacting supporters to encourage them to write to their MP or attend a public meeting or rally, would be covered by the direct marketing rules.

Our experience is that this inconsistency is confusing for data subjects and for organisations who wish to communicate with their existing customers, members or supporters. For example, as a charity we (or our trading entity) could make use of the soft opt in on our online shop or for our paid events, but we are not able to if someone downloads a fundraising pack, which is free, or if they make a donation.

We also feel that the phrase 'soft opt in' is misleading – in practice it is an opt out model of gaining marketing permission, with much in common with how an organisation is able to rely on the legitimate interests condition for non- electronic forms of marketing. I.e. the individual is informed that they will receive marketing, unless they opt out. The organisation is then able to send them marketing which they would reasonably expect based on their previous interaction, which could be a purchase, a donation, becoming a member, volunteering time, or a request for information.

Our user research into marketing permissions has consistently shown that most supporters feel that marketing via electronic means is less intrusive and/or wasteful than post or phone and would be more comfortable with an opt out for email than for non-electronic methods where we are able to rely on legitimate interests. Supporters are also able to better understand a model where all channels are on the basis of an opt out, rather than a model where some channels are opt in and others opt out, as has to happen now for an organisation to rely on the legitimate interests condition for phone and post.

We support the changes suggested to the 'soft opt in' exception but would also ask that the Government takes this as an opportunity to review why electronic marketing is treated differently than traditional channels and whether that is still proportionate and appropriate.

We would also like to address the comments made by the ICO at paragraph 95 of its response to this consultation. We felt it was the intention that the Government's proposal to extend the soft opt in to cover both charities and political parties, including fundraising requests. We do not believe that there is evidence to support the ICO's assertion that additional safeguards might be required for marketing of this nature, or that charity marketing is more likely than that sent by other sectors to cause distress or significant harm to vulnerable people.

Concerns were raised at a sector level in 2015/6 and since then individual organisations, the Fundraising Regulator and Chartered Institute of Fundraising have taken additional steps to ensure that donors are treated fairly, including identifying potentially vulnerable individuals and preventing further fundraising approaches. In addition, the Charities Act 2016 requires written agreements with professional fundraisers and commercial participators to include information on how they would protect vulnerable people and other members of the public from unreasonable intrusion to their privacy, unreasonably persistent approaches or undue pressure to donate.

The fundraising preference service provides a central service for individuals to stop marketing from charities, including via email and the Fundraising Regulator is in place to ensure that complaints about unwanted marketing are dealt with appropriately.

We would therefore suggest that there are already significant safeguards in place for charities – and more than there are for other sectors**. To exclude charities from being able to take advantage of the more cost effective nature of email marketing on the same basis as commercial organisations would be punitive.**

CRUK supports the Government's ambition to cut down on the number of nuisance calls, but we have concerns that some of the suggestions could have unintended consequences for organisations and consumers.

In terms of the 'duty to report' on communication service providers, we assume that in practice this would be based on the volume of calls made from one organisation, given that the service providers would not have access to individual's preferences, or know what kind of call was being made. In June 2021 our fundraising support team made around 1,300 calls per week, but the vast majority of those were not unsolicited direct marketing. We would be concerned that calls of this kind might look like nuisance calls based on volume alone.

Any definition or trigger for reporting would need to be well considered here in order to protect the general public from those who are undertaking fraudulent activity through unsolicited calls, without inadvertently penalising those organisations, such as charities and or professional fundraising agencies, that depend on being able to make regular contact with supporters. We would emphasise that such organisations will often work hard to ensure that communication methods and frequency are appropriate and in accordance with their preferences at the time.

We are also very concerned about the proposal for services that block incoming calls from a number not on an allow list, as there is a risk that data subjects would not then receive calls that they would need to take and welcome. For example, had this already been in place, the Track and Trace service would have been largely unable to contact people. As a more commonplace example, public sector bodies, including the NHS, often call patients from unknown numbers. **We believe that this proposal fails to take into account the wide range of reasons for which organisations may contact members of the public that are not marketing.**

Further questions

We would reiterate at this point that the GDPR and DPA 2018 are largely effective legislation which whilst prescriptive in some areas also allow a large degree of flexibility. **We believe that reducing burdens on business and delivering better outcomes for people can be achieved by better education on data protection.**

We note that the ICO has a dual role of promoting best practice and enforcing legal requirements. On occasion its guidance goes above what is legally required and sets out ways of meeting obligations that can seem overly onerous, especially for smaller organisations, or where processing of data is expected and not complex.

One area that needs more explanation are the Conditions of Processing set out in Part 1 of Schedule 1 of the DPA. There are a number of conditions that could be used as an alternative to consent, but most organisations are not aware they are an option, and there is little supporting guidance to help confirm that they are appropriate to use. We do believe that bringing the UK GDPR and Data Protection Act 2018 together would be beneficial and make it easier for organisations to understand the legislation, but do not feel that it is a major obstacle that they are not.

3. BOOSTING TRADE AND REDUCING BARRIERS TO DATA FLOWS

3.2. Adequacy

In this section of the consultation, the Government asked about the UK's future approach to data adequacy decisions. The questions most relevant to CRUK include those that consider whether adequacy decisions should be risk-based and focused on outcomes; whether decisions should be made based on groups of countries, regions and multilateral frameworks as opposed to country by country; and proposed alterations to the monitoring of adequacy regulation.

International collaboration is critical to the UK's research efforts to improve cancer outcomes. Indeed, 42% of CRUK's clinical trials are international and they are underpinned by cross-border flows of personal data. The international effort in many clinical trials is particularly vital for people affected by rare or childhood cancers, as their small patient populations require researchers to recruit participants from multiple countries in order to run viable studies that improve health outcomes through innovation.

Additionally, international collaboration is increasingly important as we strive towards precision medicine. The precision medicine paradigm aims to stratify patients with common diseases into ever smaller groups based on their specific disease biology. Precision medicine is especially promising for optimising the prevention, diagnosis and treatment of cancer. However, the need to stratify patients means that, for research studies of precision medicines, large numbers of patients must be screened to find a suitable (but still small) cohort of participants. Due to this high-screen, low-eligibility dynamic of recruitment to precision medicine studies, it is widely accepted that international collaboration, where patients are recruited across multiple countries, is invaluable for screening and recruiting enough participants. Consequently, our ability to leverage the full potential of precision medicine for research and standard of care purposes will be contingent on a data regime that is conducive to this international scientific collaboration.

As an organisation, we also engage with suppliers and partners in countries where there are not currently adequacy agreements, particularly with the United States. The requirement to add additional safeguards and undertake Transfer Risk Assessments is increasingly burdensome, and we recognise that it would be beneficial to CRUK if more countries were considered adequate. Examples include event registration and virtual conferencing software, workplace efficiency technologies and offshore technology support.

A risk-based approach to adequacy regulations

Given the importance of international data flows to cancer research, CRUK agrees that a risk-based approach to negotiating future UK data adequacy agreements could be more pragmatic and better able to identify, prevent and mitigate against risks to data rights, especially those of patients enrolled in international research. However, the consultation's proposals for how to achieve this approach leaves two open questions that need to be answered before we can make a full evaluation of a risk-based approach to data adequacy.

First, there needs to be clarity on how this risk would be defined, measured and evaluated. Specifically, how will risks be identified when considering potential data adequacy decisions, and how will the likelihood of these risks and the severity of their outcomes be projected when evaluating data adequacy agreements? Given the complexities of negotiating bilateral and multilateral international agreements – arising from diplomatic relations, differing cultural and

political contexts, and variances in data law – it is critical that these risk management processes are rigorous and transparent. **We recommend DCMS share further information on its current proposals for these processes, including who would be responsible for implementing and overseeing them.**

Second, what role will stakeholders outside the UK Government have in the processes for considering, evaluating, and negotiating data adequacy agreements? Whilst strong stakeholder engagement will be important across all sectors that are affected by cross-border data flows, it is particularly vital to the life sciences sector because of its diverse composition – industry, universities, medical research charities, and governments – and use of international collaboration, for instance CRUK's own Cancer Grand Challenges programme.

We are particularly interested in learning more about the role non-government stakeholders will play in the Procedural Stage outlined in the consultation, as we expect opportunities for consultation on data adequacy decisions would be afforded to the public when Parliament debates proposed agreements. Additionally, we would like to know how the strategic interests that will inform the Gatekeeping Stage will be determined and whether the life sciences sector will be able to inform that process. **We recommend DCMS share further information on how it will work in tandem with stakeholders to make and oversee data adequacy decisions.**

Creating a scalable, flexible adequacy regime

As with the risk-based approach, CRUK broadly agrees that negotiating agreements with countries, regions or multilateral frameworks should be a pragmatic way to facilitate data flows between countries, which would be invaluable to international research. This approach would be particularly useful for research into rare and childhood cancers for the reasons described above. As such, harmonisation of data safeguards through data adequacy agreements would facilitate the cross-border data flows that are vital to delivering these studies, whilst avoiding the need for costly and complex additional safeguards.

However, and again like the risk-based approach, we have two questions regarding how multi-country data adequacy decisions would be made in a practical, responsive and responsible way:

1. If adequacy agreements are negotiated with groups of countries, how would DCMS monitor for and respond to risks to data adequacy that emerge within an individual country in that group?
2. How would variances between countries (e.g. in how they implement a harmonised data framework) be considered when evaluating groups of countries through the process detailed in section 245?

Altering monitoring processes for adequacy regulations

Although CRUK is not opposed to moving towards a more flexible and proportionate system of monitoring data adequacy agreements, DCMS would need to provide much more information on how this system would operate for us to offer a full evaluation. As mentioned above, we are particularly interested to learn more about how stakeholders outside of government would be involved in the new data adequacy regime, including the monitoring of data adequacy agreements. This is especially imperative to the life sciences as clinical trials take many years to set up, reach

conclusions, publish and change outcomes for people with cancer across the world. We must therefore avoid creating unnecessary risks to existing and future trials.

We recommend that DCMS provides further details on its proposed process for identifying, highlighting and responding to developments that would prompt a review if the requirement to review agreements every four years is removed. In particular, we would welcome information on what events (e.g. dissolution of a data regulator) would trigger a review, and who would be responsible for deciding if an event or trend were significant enough to necessitate a review.

3.5. Derogations

Repetitive use of derogations

As a charity we do make some limited use of the derogations, and would welcome clarity around using these where the processing is not occasional. An example of this is where we provide research funding alongside an international organisational, which because they are publicly funded cannot agree to all the terms in the Standard Contractual Clauses. We ask all researchers applying for these grants to consent to the transfer, without which both funders would not be able to assess the application. Where all the other safeguards set out in Article 49 are met, it seems unnecessary to bar the use of the derogations because the transfer happens more than once.

For more information on this submission, please contact: **Sarah.cook@cancer.org.uk**