Hogan Lovells International LLP
Atlantic House
Holborn Viaduct
London EC1A 2FG
T +44 20 7296 2000
F +44 20 7296 2001
www.hoganlovells.com

19 November 2021

By email

Dear Sir/Madam

Response to the UK government's proposal to reform data protection law

We are responding to the UK government's proposals outlined in the white paper published by the Department for Digital, Culture, Media & Sport titled 'Data: a new direction'.

Our overall view informed by many years of practising in this area and our global perspective of data protection law is that the success of the proposed reform to the current regime lies in the government's ability to strike the right balance between a progressive and realistic new framework, and the need for consistency with the global approach to the protection of privacy and personal data. We believe that this objective is possible and that the UK has an influential role to play in this respect.

Set out below are our comments on a number of principal areas of the consultation which we consider to be of particular importance. To summarise:

1. We support the UK government's efforts to encourage greater innovation, through making specific and targeted changes to data protection law, including with respect to the processing of personal data for scientific research and development purposes.

2. The introduction of a set of purposes which are automatically assumed to be within the legitimate interests of a controller has the potential to be helpful. There are a number of additional purposes that we have also suggested as additions to this list.

3. While it is important that outcome fairness in an AI context is addressed through regulatory reform, there are a number of drawbacks to relying on the UK GDPR as the basis for introducing these obligations, compared with introducing separate, dedicated legislation.

4. The current rules governing solely automated decision-making are too prescriptive and could be reformed by removing certain restrictions on the use of these technologies and requiring better oversight, while protecting the existing rights afforded to data subjects.

5. Introducing a statutory definition of 'anonymisation' is a sensible proposal and would provide much-needed clarity. Incentives should also be provided for organisations to proactively adopt privacy-enhancing technologies.

6. There is a risk that the proposal to replace the existing accountability framework could be perceived within the EU's institutions that the UK is seeking to lower standards. This may be a factor in the European Commission's determination of whether to renew the UK's adequacy status in 2025.

7. The existing cookie consent framework does not work for either businesses or users and is detrimental to the digital economy. However, moving away from a consent-led approach to cookies is inherently complex and needs to be seen as an iterative process, as opposed to a revolution. There are various immediate changes that could be made to help achieve this.

8. We agree that the current approach to adequacy assessments can be overly prescriptive and inflexible and the objective should be to increase the free flow of personal data across borders. However, changes to the rules on adequacy will not succeed without collaboration and consensus between the UK and other countries and institutions.

9. The field of international data transfers has become increasingly complex over recent years. These complexities need to be overcome through greater standardisation of the existing rules and requirements, which the UK government can help to facilitate through various targeted measures.

1. Scientific research purposes

1.1 Encouraging the performance of scientific research and the development of emerging technologies is of significant importance to the future of the UK economy, and indeed the world's. Given the integral role that personal data has in these areas, it is crucial to have a data protection framework that is easily understood and facilitates both public and private research and development initiatives, particularly those that are in the public interest.

1.2 We therefore welcome the UK government's proposals to simplify and clarify the principles and obligations that apply to the processing of personal data in this context. The introduction of a new definition of 'scientific research' has the potential to help researchers and privacy practitioners better understand the scope of activities that are subject to certain rules and exemptions under existing data protection law. Similarly, creating a new lawful basis for processing that is connected with scientific research, and clarifying the rules governing the reuse of personal data for such purposes, would be helpful additions to the UK GDPR.

1.3 If constructed appropriately, then this addition has the potential to remove uncertainty and, as a consequence, further incentivise commercial research while also encouraging greater collaboration and innovation between organisations.

1.4 In order for these benefits to be fully realised, we would like to emphasise the importance of the reforms addressing the following areas:

- The new definition of scientific research should be drafted so that it is clear that socially beneficial commercial research falls within its scope, including the development of new technologies or the improvement of existing ones.

- In addition to the new lawful basis under Article 6 of the UK GDPR, a suitable condition is also incorporated into the Data Protection Act 2018 to facilitate the processing of special category data for the same purposes, subject to appropriate safeguards.

- Significant collaboration is often required between public and private organisations, alongside independent researchers (e.g., in order to perform peer reviews). It is therefore important that it should be made clear that, where it is necessary to share personal data for these purposes, then such sharing will be permissible and supported by the new 'scientific research' ground for processing under Article 6 of the UK GDPR.

2. Legitimate interests

2.1 The proposal to create a limited and exhaustive list of legitimate interests for which organisations can use personal data, without applying the balancing test, has the potential to provide helpful clarification for business and reduce the regulatory burden in a proportionate manner.

2.2 With this in mind, and based on our experience of advising businesses on this issue over many years, we suggest supplementing the current list of proposed processing activities, that would fall within this exemption, in order to include the following:

- Performing compliance checks, including those that are necessary for KYC purposes, such as anti-money laundering, anti-fraud and sanctions checks.

- Verification of an individual's identity.

- Reporting of alleged regulatory infringements, which are of a civil (as opposed to criminal) nature, to the relevant authorities.

- Sending servicing communications to customers and other individuals, which do not constitute marketing.

- Sending business to business communications, including for marketing purposes.

- Sharing personal data with other controllers within the same group of companies.

- Sharing of personal data with other third parties in relation to the sale or acquisition of the rights or interests in a legal entity.

- Performing equality and diversity assessments.

- Undertaking performance reviews and assessment.

- Product development and improvement.

2.3 In addition, the UK government should ensure that each of the identified processing activities are, where relevant, complemented with appropriate exemptions for processing special category data under Schedule 1 of the Data Protection Act 2018. For instance, the current insurance exemption under Schedule 1 of the Data Protection Act 2018 is insufficiently broad, meaning that insurers are currently unable to improve their existing pricing and claims models in a way that would allow them to offer more bespoke products which align with customer expectations.

3. Fairness in AI

3.1 The UK government is right to identify that the application of the fairness principle in the context of AI and machine learning systems is currently unclear. We also acknowledge that ethical concerns relating to 'outcome fairness', such as the potential for algorithmic bias, are important and need to be clearly addressed under the UK's regulatory framework that applies to these technologies.

3.2 However, there are a number of limitations of introducing an explicit requirement under the UK GDPR for AI systems to be developed in a manner that ensures the fairness of outcomes for individuals. These include:

- The UK GDPR is generally considered to be a technology-neutral regulation which is intended to apply a set of principles that organisations are expected to comply with consistently, irrespective of the means by which personal data is being processed.

- There are often complex supply-chains involved in the design, development and use of AI systems. This means that the controller/processor paradigm under the UK GDPR often does not consistently align with how responsibilities for outcome fairness may need to be allocated in practice.

3.3 For these reasons, we encourage the UK government to consider introducing outcome fairness obligations through separate legislation, which is enacted as part of the wider National AI Strategy.

4. Automated decision-making

4.1 While there is guidance that has been provided on the application of the rules relating to solely automated decision-making under Article 22 of the UK GDPR, amongst some organisations its application is still not well-understood. Equally, the present approach of seeking to limit the use of algorithmic technologies in circumstances where they are solely automated and have a legal or similarly significant effect, is overly prescriptive and, in practice, does not adequately take into account the risks and outcomes that such decisions may have on the fundamental rights of data subjects.

4.2 Therefore, while we consider that Article 22 forms an important component of the UK data protection framework, we also see the need for reform. Our recommendations are as follows:

- The general restriction on solely automated decision-making (Article 22(1)) the exemptions to this restriction (Article 22(2)) and the additional restrictions on the use of special category data (Article 22(4)) should be revoked, with the emphasis instead being on controllers having a lawful ground for processing the personal data under Article 6 of the UK GDPR.

- A new obligation should be introduced, either under Article 22 or through separate legislation, which requires systems that involve solely automated decisions being taken about individuals, to be subject to an appropriate degree of human oversight. This oversight would be intended to ensure that such systems are performing as they are expected and not creating risks to the rights and freedoms of data subjects.

- In addition, the existing right for data subjects to obtain human intervention, express their point of view and contest the decision under Article 22(3) should be retained.

5. Data minimisation & anonymisation

5.1 The proposal to include a statutory definition of 'anonymisation' is sensible and should provide much-needed clarity on when data is considered to fall outside the scope of the UK's data protection framework. It is important that any new definition acknowledges that whether data is considered anonymised is relative to the circumstances. Equally, where pseudonymised personal data is shared with a third party that does not have any reasonable means of accessing the original 'key' or re-identifying the data set through other methods, then the law should also clarify that such data should also be considered to be anonymous. This should help to facilitate the sharing of data sets between organisations, in accordance with the government's wider data strategy.

5.2 Privacy-enhancing technologies (PETs) should be encouraged both through the data protection framework and by the ICO. This includes pseudonymisation, but also emerging technologies such as differential privacy and federated learning. One example of how this could be achieved, is by UK data protection law specifically acknowledging that processing of personal data through the use of PETs will not be considered high risk to the rights and freedoms of individuals, where the purpose does not involve profiling or making decisions about specific data subjects. This type of provision also has the potential to foster greater innovation.

6. Accountability

6.1 We acknowledge and recognise the UK government's concern regarding the administrative burden placed on businesses as a result of the UK GDPR's existing accountability framework. This burden can be particularly onerous for small and medium-size enterprises (SMEs) and other organisations that do not have the resources to appoint a DPO or perform regular DPIAs.

6.2 Nonetheless, the existing accountability framework, while still under development in practice, is also well-understood by the majority of organisations. Many organisations have dedicated considerable resources both before and since the GDPR first took effect in May 2018 to develop internal governance programmes that meet the current standards. This is a worldwide phenomenon that is taking place across many different legal cultures that are beyond the scope of application of the GDPR. Therefore the introduction of a new Privacy Management Programme (PMP) requirement needs to be carefully considered against this background.

6.3 Equally, the proposed reforms could potentially give rise to the possibility of diverging standards of accountability between the UK and other jurisdictions that follow the GDPR model. Any degree of divergence that causes inconsistencies among various standards could ultimately be problematic for many organisations (both large and small) that operate across borders, who currently have in place privacy programmes which are implemented in order to comply with various regimes.

6.4 The current proposals, such as removing obligations to perform DPIAs, appoint a DPO and maintain records of processing, may potentially also create the perception within the EU's institutions that the UK is seeking to lower the standards of accountability. This could be a factor in the European Commission's determination of whether to renew the UK's adequacy status in 2025 and therefore the government should take into account this risk.

6.5 We therefore recommend that the UK government puts forward a targeted and balanced set of reforms to the accountability framework. These reforms should seek to address some of the

current weaknesses of the existing regime, while mitigating the risks that have been identified above.

6.6 Being more specific, we welcome the suggested increase to the threshold for personal data breach reporting and also the voluntary undertakings process that has been put forward. Putting in place proportionate controls to discourage the malicious or speculative use of DSARs is equally sensible, subject to ensuring that it does not discriminate against individuals who have more limited financial means.

6.7 To address one of the government's concerns, we also believe there is opportunity to make compliance easier for SMEs. For instance, this could involve introducing specific exemptions for appointing a DPO and maintaining records of processing.

7. Cookies

7.1 The use of cookies and similar technologies, particularly as part of the digital advertising ecosystem, continues to generate much debate and sometimes controversy. However, what can sometimes be overlooked in these discussions is that the existing cookie consent framework is not fit-for-purpose.

7.2 The current obligation for operators to obtain prior GDPR-standard consent for such a broad range of online processing activities creates a considerable nuisance, has significantly disrupted the way in which websites, mobile apps and digital platforms operate and ultimately done little to protect the privacy of individuals. Equally, for many businesses, particularly free online services that rely on digital advertising to generate revenues, the existing consent framework has the potential to pose a threat to their survival.

7.3 While the intention to protect users is both valid and important, there is a need for the current rules to be reformed so that they are more risk-based, proportionate and incentivise privacy-enhancing solutions, rather than being overly prescriptive consent requirements.

7.4 However, moving away from a consent-led approach to cookies is inherently complex and needs to be seen as an iterative process, as opposed to a revolution. The UK government will need to work alongside industry and other governments if these reforms are to be successful and we would be happy to help to facilitate such engagement. This is necessary in order to ensure that there is broad international consensus on how to resolve the current inadequacies and there are appropriate technological solutions in place to ensure that user privacy can be adequately protected online.

7.5 In order to address these challenges, we recommend that the UK government takes the following steps:

- As suggested in the proposal, the scope of the current 'strictly necessary' exemption should be expanded to include analytics cookies. It is important that this exemption expressly includes both conventional cookie-based technologies that are utilised through websites, but also other similar technologies that may be adopted in mobile apps.

- The existing consent obligation under Section 6(3) of the Privacy and Electronic Communication Regulations should be amended, so that the need to obtain consent only applies where the storage or access to information is likely to result in a risk to the rights and freedoms of data subjects.

- Ways in which the accelerated adoption of privacy-enhancing technologies can be incentivised should be further explored. This could include permitting alternative lawful grounds for processing to be relied upon by operators, instead of consent, where PETs are utilised in a manner that protects the privacy of the user.

8. Adequacy decisions

8.1 We agree with the UK government's observation that the current approach to adequacy assessments can be overly prescriptive and inflexible. This has sometimes resulted in third countries not receiving adequacy status, despite in practice having equivalent standards of data protection as those that are present within the EU and UK.

8.2 The objective should be to increase the number of adequacy decisions that are granted, in the interests of promoting and facilitating the free flow of personal data between countries while retaining the credibility in the adequacy determination process. Therefore, we encourage the UK government and ICO to work with other countries in developing a more risk-based and outcomes-led approach to adequacy decisions. This could include, for instance, looking at how adequacy decisions could be granted to specific industry sectors within a jurisdiction, which have higher standards of privacy protections in place (e.g. the healthcare and financial services sectors in the United States), rather than focusing on an all-or-nothing approach.

9. International data transfer mechanisms

9.1 Recent developments in the field of international data transfers, both within the UK, EU and elsewhere, have created an increasingly complex environment for organisations to operate within. It is therefore paramount that the UK government explores opportunities to collaborate with other governments across the world to develop more consistent global standards for facilitating the free flow of personal data.

9.2 At a domestic level, we believe that the real benefits for organisations would come from greater standardisation of the current transfer mechanisms, alongside the introduction of alternative safeguards that are based on the same principles and achieve the same objectives. Immediate priorities should include:

- Confirming in law that, subject to any necessary and limited amendments, the current EU standard contractual clauses can be utilised as a valid appropriate safeguard for transferring personal data from the UK to the EU.

- Encouraging the ICO to provide organisations with written confirmation of the UK's view on the standards of protection offered to data subjects in other third countries and, where the standards fall below what is expected (in accordance with the *Schrems II* ruling), then what specific supplementary measures need to be implemented to facilitate the lawful transfer of personal data to that country.

- Exploration of how codes of conduct (as envisaged under Article 40 of the UK GDPR) could be utilised to facilitate transfers of personal data between companies that are not within the same group.

Conclusion

Today's global data protection law is not set in stone. It is constantly evolving as it has been for over more than 40 years. Some of that evolution involves re-writing laws and regulations and

some of it requires undertaking a dynamic interpretation of the existing framework that is able to adapt to technological and societal changes in order to achieve the necessary objectives. Where appropriate, the UK government should engage with stakeholders in the sector for assistance in developing the legislation, and make use of the ability to interpret the current law flexibly and pragmatically so that suitable adaptations can take place without necessarily changing the black letter of the law.

To the extent that greater certainty or a more effective legal framework is required, legislative reform should be undertaken by exercising global leadership in order to promote consistency across jurisdictions to address a global need. Both citizens and organisations will benefit greatly from this approach in the UK and beyond.

This is ultimately an opportunity for the UK to lead the way in designing the most effective data protection regime in the world, which protects individuals while unlocking innovation and growth in the digital economy, so we encourage the UK government to engage internationally in this process and promote a collaborative and progressive outlook to the regulation of the use and protection of personal data.

Yours faithfully

Hogan Lovells International LLP