Memo to the Minister on Data Law Reform from
The Privacy Laws & Business/ Norton Rose Fulbright Roundtable

Dear DCMS Minister Matt Warman MP,

This *Memo to the Minister* provides you with the recommendations made at the Privacy Laws & Business/ Norton Rose Fulbright Roundtable on 14 July before the Data Protection and Digital Information Bill was published. However, the points of substance below remain valid as much of the substance remains in the Bill.

We were lucky enough to have had questions relating to the then forthcoming Data Reform Bill answered by DCMS representatives, Elisabeth Stafford, Robin Edwards, Emily James and Gaby Anderson at the Roundtable.

The DCMS team were very knowledgeable and the participants (generally data protection experts from UK businesses and private practice law firms) were given a good insight into the rationale for the Data Reform Bill changes. Some of the participants' comments were new and valuable for the DCMS staff.

The attached minutes provide the full set of questions asked and responses given by the DCMS representatives. We have extracted the following highest priority points meriting your further consideration as the Data Protection and Digital Information Bill progresses through Parliament.

REDUCING BARRIERS TO RESPONSIBLE INNOVATION

1. There are concerns that the Data Reform Bill will not have sufficiently wide gateways to allow data sharing for financial crime (fraud, AML) investigation purposes in connection with the Economic Crime Bill.

2. Is the government considering creating a class of private sector organisations subject to similar obligations as "data intermediaries" under the EU Data Governance Act with fiduciary duties that can be enforced by regulators that individuals can trust to hold and police special category personal data provided to AI developers to monitor and correct bias in AI systems? There are many examples of well-intentioned Diversity & Inclusion programmes hanging onto this data beyond the initial research question with the intention of showing improvement over time – unfortunately increasing the risk of misuse, rather than fixing it, so the creation of a regulated intermediary may be a good solution.

3. Only a third of respondents to the consultation agreed that the UK GDPR definition of research represented "a clear and broad base that was understood by researchers." The remainder did not consider that it was suitable, or were undecided. Given that Recital 159 is very wide and the government is relaxing various other safeguards (e.g. broad consent; requirement to provide fair processing information), would a clearer definition of research be appropriate rather than leaving this to the ICO and/ or the courts to determine?

4. The Data Protection Act 2018 provides for an exemption for some of its requirements where "personal data is processed for the purposes of approved medical research" defined as research approved by a Research Ethics Committee (REC) or equivalent body. Each of those bodies has threshold criteria. This results in a body of medical research that is not

"approved medical research" on the basis that it does not represent a sufficient risk to meet the criteria triggering the requirement for a REC review.

This creates the somewhat perverse position that, even though the medical research is considered sufficiently "low risk" not to require REC approval, the research body cannot rely on the DPA research exemption by virtue of the fact the research has not been subject to the approval it does not require. Will the new law clarify whether medical research can be treated as "approved medical research" on the basis that (1) it is being undertaken by a body that is subject to duties of confidentiality and (2) all requirements to seek approval have been met, by virtue of the fact that none of the triggering criteria are engaged?

5. The government plans to legislate to provide further clarity on the distinctions between "new" processing and "further" processing. Has a decision yet been made as to whether processing by a new controller (for example, in order to leverage the specialist skillset of that controller) amounts to new processing or further processing? An example is sharing an NHS database relating to dementia outcomes with a private pharma company.

REDUCING BURDENS ON BUSINESSES AND DELIVERING BETTER OUTCOMES FOR PEOPLE

6. The majority of respondents disagreed with the proposal to remove a Data Protection Officer (DPO). However, the government is proceeding with the proposal to replace the DPO with "a responsible individual(s)", which does not need to meet the specific requirements/responsibilities of a DPO under the UK GDPR, including independence:

    6.1. Is the renaming of this function really necessary? Surely, it would be better to retain the well-known term "Data Protection Officer" understood by both large and small organisations?

    6.2. If a company retains a DPO (required by the EU GDPR) and also appoints a senior person as the "Responsible Individual", might that cause tension over the independence of the DPO and a possible conflict? To give more context:

        6.2.1. For larger organisations, senior management do not, on the whole, have the necessary expertise to advise the organisation on DP requirements. This is particularly the case where organisations have complex data processing eco-systems, use/build AI, process particularly sensitive data with vulnerable individuals etc.

        6.2.2. Senior management certainly do not have sufficient time to dedicate themselves to this role on top of their other roles.

        6.2.3. For smaller organisations, there will more often than not be a conflict of interest, given that senior management will already have multiple other roles that they have to fulfil. So they will end up having to delegate anyway.

        6.2.4. In practice, larger organisations will have to keep the DPO role but impose on a senior individual additional responsibility as well. For smaller organisations, the good ones will recognise that they still need external support with this role so will not be in any better position. The bad ones, will appoint a senior person who will not have sufficient time/expertise to do the role and will end up in a worse compliance state

Does this possible conflict need to be addressed through dropping the "Responsible Individual" role, or clarification in the Bill, or left to guidance from the ICO?

DPOs have paid a critical (and vastly under-rated) role in making sure privacy is on the agenda for their organisations and is given proper consideration. Getting rid of this role will devalue the importance of data protection in many organisations and will undermine the good work that has been done to date under GDPR.

7. In relation to the changes to abuse of data subject rights, the word "vexatious" is currently used in the Freedom of Information Act and there has been significant case law and guidance on its interpretation which, in practice, such that it may not change the threshold (i.e. will it make much difference in practice?). Would clearer drafting be more appropriate here?

8. Relating to the "excessive" part of the threshold, the key change with excessive is that "manifestly" is coming out from beforehand. Will this also impact the "excessive" threshold (i.e. "manifestly excessive" vs "excessive"). Will any practical examples be given of the difference, if any, intended here?

9. Some commercial organisations offer free products (e.g. webinars, samples, downloads, conferences etc.) when they collect prospects details for the first time or offer free services (often funded by advertising (e.g. certain dating services) or through commission paid by product providers (e.g. price comparison services)) and are reluctant to rely on the soft opt-in since this currently requires a "sale" or negotiation for a "sale", which suggests monetary consideration needs to be sought/ paid. If the soft opt-in is to be extended to non-commercial organisations on the basis of a "previous relationship" for charities/ political parties, this suggests that non-commercial organisations will be able to rely on a broader application of the soft opt-in that commercial organisations. Should the soft opt-in be extended to commercial organisations to allow them to benefit from this where they have a similar "previous" relationship as opposed to a sale/negotiation of sale?

10. The government has confirmed that "organisations that are currently compliant with the UK GDPR would not need to significantly change their approach to be compliant with the new requirements". Organisations which have already made substantial investments in their GDPR compliance programmes are understandably keen for clarification that they will not need to make any changes - . or if that is not the case, clarification on the specific areas where changes are mandatory. Could this be addressed through a clarification in the Bill, or will it be addressed in guidance from the ICO?

BOOSTING TRADE AND REDUCING BARRIERS TO DATA FLOWS

11. From a privacy perspective, businesses appear to be keener on preserving the EU's adequacy finding in respect of the UK than the UK awarding adequacy to other countries. This position applies particularly if the transfer risk assessment process that accompanies the use of SCCs can be streamlined or facilitated by the legislation in a way that does not also tempt the EU to withdraw UK adequacy.

12. The Roundtable participants advocate the UK government continues its very close coordination with EU counterparts on this point rather than softening the approach on either point too quickly and provoking further uncertainty on the EU's adequacy finding in respect of the UK.

13. Any UK adequacy finding in relation to a third country will be immediately used by EU lawyers trying to justify exports to that country in their transfer impact assessments. This may mean that an EU statement on any perceived flaws or weaknesses in the decision could follow very swiftly with privacy activist litigants supporting this argument by taking collective action though the courts.

REFORM OF THE INFORMATION COMMISSIONER'S OFFICE (ICO)

14. There is a concern regarding the unspecified allocation of costs of technical reports that may be commissioned by the ICO. Whilst businesses would like certainty in this area, they would also like to see safeguards around where reports have already been commissioned and expense incurred, that this cost and effort does not have to be duplicated through the preparation of an ICO technical reports.
15. Businesses have expressed concern about how the production of expert reports for the ICO could be used in proceedings in other jurisdictions where such reports would not normally be provided and would be subject to legal privilege. The legislation should provide some clarity in this area and how legal privilege can be maintained.

We would be most willing to discuss any of these points with you or your colleagues.

Yours sincerely,

Marcus Evans, Partner, Norton Rose Fulbright Marcus.Evans@nortonrosefulbright.com

Stewart Dresner, Chief Executive, Privacy Laws & Business stewart.dresner@privacylaws.com

28 July 2022