Bates Wells Braithwaite

10 May 2017

By email:

Dear Sir or Madam

DCMS call for views - GDPR

1. **Background**

1.1 Thank you for giving us the opportunity to participate in this consultation.

1.2 Bates Wells Braithwaite is a professional services consultancy, combining a top legal practice with services in impact measurement, outcomes-based planning and strategy, and financial services regulatory compliance. It is not only recognised as the leading charity law firm in the UK; it is ranked in the major UK legal directories for its excellence across many of its specialist practice areas. As part of this offering, it has a significant data protection practice.

1.3 Given the broad nature of the consultation questions we have provided some responses below that we deem to be particularly pertinent to our clients and their work. However, this is not an exhaustive statement of our views on the derogations in GDPR and we would welcome the opportunity to comment on any proposals or draft legislation which government puts forward.

2. **Theme 8 – Criminal Convictions**

2.1 We note that Article 10 (criminal convictions and offences) is expressed in such a way that EU or Member State law will generally be required to provide legitimate grounds for the processing of this type of personal data.

2.2 A number of our clients process this kind of data for different reasons (including, but not exclusively for, their employment purposes), and we would suggest that the UK uses its authority under Article 10 to provide a reasonable and proportionate means for them to continue this processing: for example, to broadly reflect the Data Protection Act 1998 and provide that Article 10 (criminal) data may be processed as long as the regime for sensitive personal data is complied with, and, insofar as this is possible, promoting suitable and sufficient exemptions elsewhere in GDPR for processing of data for the purposes of the prevention and detection of crime, and for employment purposes in accordance with the current law.

3. **Theme 10 – Processing of Children's Personal Data by Online Services**

3.1 Under Article 8, a Member State may reduce (from 16 to as low as 13) the age at which the consent of a parent or guardian is required where consent is to be relied upon as a basis for providing “information society services”.

3.2 We suggest that government provides further information on its position to enable respondents to provide views in this area. We note that in practice many under-16s are largely or entirely autonomous or unsupervised in relation to online activity, and would welcome guidance on the kind of practical mechanism which bodies could put in place, to provide “reasonable efforts…taking into consideration available technology”, to ascertain that the consent of a parent/guardian has been obtained, as is required by the Article. We would specifically welcome a statement from government acknowledging that the level of technology which is “available” depends on an organisation’s resources. A small non-profit organisation, for example, may have significantly less resource to divert to invest in the latest technology.

4. **Theme 12 – Processing of Data**

4.1 There are a number of relevant derogations applicable in this theme. For present purposes we wish to comment on article 6 (which sets out the conditions for processing), and provides a Member State with (among other things) the ability to provide further detail to ‘adapt’ and set out in domestic law the basis for processing in respect of the following conditions:

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4.2 We note that the ‘legitimate interests’ condition is expressly stated not to apply to public authorities and would suggest that headings (c) and (e) are made commensurately broad. It is essential that public bodies are able to conduct their legitimate day-to-day functions, as determined by Parliament, without undue legal expense or effort to justify the processing as falling within another condition. It is also appropriate to ensure that bodies which work with public authorities (and those which share data with them), including a significant number of our clients, can operate with confidence that the arrangement is compliant where the public authority is pursuing its functions and the partner body is acting in its legitimate interests. In our view it is essential that the government provides a clear legal and sufficiently broad basis to legitimise processing by public authorities.

5. Article 88 also provides that a Member State may provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context. Given the apparent tightening up of the rules in respect of employee consent and the uncertainties other exemptions will cause it is important that the UK provides specifically that employers can have an accessible and legitimate ground to process employees’ (and workers’) personal data.

6. **Theme 14 - Rules surrounding Churches and Religious Associations**

The derogation in Article 91 states that churches and religious associations which apply comprehensive rules “relating to the protection of natural persons with regard to processing” within a Member State may continue to apply them “provided that they are brought into line with this regulation". We understand this to be somewhat circular: surely any data controller

can apply any kind of rules which are in accordance with GDPR. We would welcome government's views on the practical application of this article and any domestic provisions which it is proposing to adopt in relation to it.

7. **In the context of the derogations above, what steps should the Government take to minimise the cost or burden to business of the GDPR?**

7.1 As stated above, in addition to advising businesses, we act for a very large number of charities and social enterprises. Like certain businesses, a significant proportion of third sector bodies need to process significant quantities of personal data to operate or continue in business at all. For example, many charities receive their income primarily or exclusively from public fundraising, as well as managing employees and volunteers on a daily basis.

7.2 Government should be cognisant that charities and non-profit entities, particularly smaller ones, can have significantly fewer resources to implement changes to their compliance processes and procedures to comply with new law. Additionally, charities of any size are generally run by volunteers, and rely on volunteers to operate. As bodies answerable to the public working in areas providing vital services, they can also encounter public pressure to increase the proportion of funds spent directly on their beneficiaries, and reduce the proportion spent on 'overheads' such as legal advice or (to take the example above) age verification mechanisms. We consider that the UK should take this into consideration when exercising its discretions under GDPR.

7.3 In particular, we note that until there is certainty about the UK's position on the issues raised in this consultation, there are significant 'grey areas' in the incoming law which organisations cannot begin to prepare for. We would therefore recommend that whenever it is within the government's discretion, generous transitional periods are put in place before any new provisions are introduced. In particular, where it is proposing to introduce a regime under a derogation which is more restrictive than the current law, that regime should provide that compliance with the current law is also permissible for a fixed period of time.

8. As mentioned above, we are grateful for the opportunity to provide comments and would welcome the opportunity to comment further on government's proposals for derogations in due course.

Bates Wells Braithwaite