



Department for  
Digital, Culture  
Media & Sport



Home Office

TO2017/06038/DC

19 October 2017

My Lords

### **Data Protection Bill: Second Reading**

We would like to renew our thanks to all Peers for a very useful debate at the Second Reading of the Data Protection Bill. As we feared, we were not able to respond to all of the many important points raised in the time permitted and hope to cover those points in this letter.

#### Bill complexity

We share many Peers' regret that it is not possible to copy out the GDPR, or otherwise annex it to the Bill, to improve readability. However, a copy of the Regulation is available from GOV.UK at

<https://www.gov.uk/government/publications/data-protection-bill-general-processing>

A Keeling Schedule, showing a comparison of the GDPR and applied GDPR, is available from the same page.

A number of unofficial websites providing more interactive versions of the GDPR are also available. We understand that, rather appropriately, there is even an unofficial GDPR 'app' available for mobile devices. We do stress, however, that these are unofficial resources.

Prior to the debate, a number of Peers suggested that, in scrutinising the Bill, it might be helpful to be able to cross-refer the exemptions provided in Schedules 1, 2 and 3 to those of the Data Protection Act 1998 (the 1998 Act). A table is annexed to this letter which Peers may find helpful.

#### Rights of data subjects

Lord Storey and the Earl of Lytton raised the issue of data controllers who might spuriously claim that a request is "manifestly unfounded or excessive" in order to avoid their transparency obligations. It is worth making a couple of points. First, regardless of whether the controller is captured by Part 2 or Part 3 of the Bill, the

burden of proof is on them to show that it is manifestly unfounded or excessive. This is a high bar and the Information Commissioner will no doubt scrutinise such claims carefully. Secondly, clauses 11 and 51(4) provide important backstop powers that will ensure the Secretary of State can act if controllers are found to be using inflated charges to prevent data subjects from exercising their rights.

Lord Knight of Weymouth raised the question of how the right to be forgotten works with blockchain technologies. Both the Bill and the GDPR, including exemptions available in relation to this and other relevant rights, are technology-neutral. The Information Commissioner's current guidance is that controllers should be clear with data subjects about what is meant by term 'deletion' and that it should normally mean that the content should not be recoverable in any way. However, the Information Commissioner has stated that she will adopt a realistic approach in terms of recognising that deleting information is not always a straightforward matter, where limitations have been clearly signalled to data subjects.

#### Assistance for data controllers

There are a couple of specific publications, referenced briefly in the debate, which may be of interest to Peers:

- *Preparing for the General Data Protection Regulation: 12 steps to take now.* Available from the ICO website: <https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf>
- *Guidance: what to expect and when.* Available from the ICO website: <https://ico.org.uk/for-organisations/data-protection-reform/guidance-what-to-expect-and-when/>

Further, a number of law firms and NGOs have also published helpful guides for both data controllers and data subjects on their rights and obligations.

One recurring theme of the guidance available is that there are often options available to data controllers to help them minimise the costs of compliance. The question of Marlesford Parish Council, raised by Lord Marlesford, is a case in point. He is right to say that every public authority will need to nominate a data protection officer. However, this does not have to be a dedicated person, and small public authorities, such as parish councils, may well be able to share data protection officers to help reduce the cost.

#### Protecting children

Lady Kidron was among those who asked how social media companies and others would be able to verify the age of individuals wishing to use their services. It will be for individual companies to demonstrate that they have made reasonable efforts to ensure they have taken the correct approach to seeking consent. At the moment, most websites start by asking questions and then investigating unusual behaviour or complaints. But this is a rapidly evolving space and one where we would expect to see some change over time. We can also reassure the noble Baroness that should firms not take their obligations seriously, they would be subject to enforcement action by the Information Commissioner, including a maximum fine of £9 million or 2% of global turnover in particularly egregious cases.

The noble Baroness also highlighted the issue of how the Government intends to protect young people from the consequences of data harvesting, especially given the often long and confusing nature of terms and conditions. We can reassure her that where processing is based on consent, the controller must be able to demonstrate that every individual data subject, however old or young, has genuinely consented to processing of his or her personal data. Moreover, if the data subject's consent is given in the context of a broader 'terms and conditions' document, the request for consent to process personal data must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

Lord Arbuthnot of Edrom and Lady Howe of Idlicote questioned the relationship between clauses 8 and 187 of the Bill. Clause 187 says that children in Scotland are presumed to have capacity to give consent to processing of data in all situations when they are aged 12 years or over. (In England & Wales, to determine capacity one must look elsewhere, normally to the common law.) Clause 8 is complementary. It sets the age under which parental consent is required for an individual's personal data to be processed at 13, but this adds to, rather than supplants, the question of capacity. Clause 8 is also restricted to processing by "information society services" (i.e., websites), whereas clause 187 – and the common law – are broader in their application.

Similarly, Lord Kennedy of Southwark and Lord Stevenson of Balmacara questioned why the right to have social media content deleted only 'kicked in' at age 18. Peers will be relieved to know that this is not the case. The right to be forgotten, of which this is one particularly important facet, is a universal right for data subjects.

#### Medical research

Lord Patel was among those who raised concern that the Bill might impede some important types of medical research where patient consent cannot be relied upon as the basis for processing. The Government is determined to ensure that the Bill does not impede legitimate medical research. We agree with Peers that medical research which is carried out by universities or other organisations for the benefit of society is highly likely to constitute a matter of public interest under article 6 of the GDPR. The list of "public interest" functions in clause 7 is not, and cannot be, an exhaustive one and we will amend the explanatory notes to make that point clearer.

Processing of personal data concerning a person's health would also need to meet a condition in article 9 of the GDPR. The most relevant condition for medical research purposes is likely to be article 9(2)(j) (processing which is necessary for scientific research purposes). As Lord Patel pointed out, however, that article must be read in conjunction with the safeguards in clause 18 of the Bill. Article 9(2)(h) and paragraph 2 of Schedule 1 to the Bill also permit processing which is necessary for the purposes of preventive or occupational medicine, medical diagnosis or the provision of health care or treatment. We look forward to discussing these issues further as the Bill proceeds to ensure there are no unintended side effects.

### Unethical use of data

A number of Peers raised the issue of the unethical use of data. As many Peers will be aware, the Government is committed to establishing a Data Use and Ethics body as ethical norms are important alongside legislation in the governance of data use. The body will develop a sound ethical framework for how data can and should be used, addressing both existing and emerging ethical issues. Its work will ensure that our regulatory and governance frameworks are responsive and effective in dealing with these issues. This will mean that the public trust that their data is being handled properly, businesses have confidence to innovate and we secure our position as the best place in the world to set up data-driven businesses.

It may be helpful to reiterate the point made in summing up that any use of personal data must comply with the relevant legal requirements. This includes compliance with the necessary data protection principles, of which purpose limitation is one. This ensures that once personal data is obtained for one purpose it cannot generally be used for other purposes without the data subject's consent.

Of course, as Lord Knight of Weymouth pointed out, data protection law is not the only relevant source of obligations in this area. The noble Lord referenced ePrivacy. As he will no doubt be aware, revised proposals on ePrivacy are currently being discussed at a European level. The UK looks forward to working with other Member States to achieve a text that strikes the right balance between protecting the confidentiality of electronic communications and promoting the data economy.

### Automated decision-making

In his opening remarks, Lord Stevenson of Balmacara referred to concerns about the use of personal data to inform automated decision making. The Government is alive to these concerns. Going forwards, there will be a number of complementary safeguards in this space for data subjects who find their personal data being used for the purposes of automated decision-making by commercial organisations. First, they will benefit from the safeguards provided for other uses of personal data (for example, tighter rules on transparency and consent). Second, they have a right to be told that their data will be used for automated decision-making and to be provided meaningful information about the logic involved, as well as the significance and the envisaged consequences. Finally, in a wide range of circumstances they will benefit from a specific right to obtain human intervention. Lord McNally, will be pleased to know that the same right to human intervention also applies in the context of processing for law enforcement purposes.

### Legacy data

The Earl of Lytton raised the issue of 'legacy data'. The short answer to his question is that there is, in general, no distinction between 'legacy' and 'non-legacy' data (although, as noted by Lord Janvrin, there are specific exemptions available to those undertaking archiving in the public interest). Personal data collected prior to the new arrangements coming into force should be treated identically to data collected after. As Peers will be aware, data controllers are already under an obligation to ensure that personal data is only held for specified purposes, is accurate and up to date, and is not kept for longer than is necessary. So they should already be aware of what personal data they hold and why they hold it. If they are not, then it should be top of their to-do list to find out.

### Money laundering

Lord Arbutnot of Edrom asked whether financial institutions making suspicious activity reports under the money laundering regulations constituted part of the law enforcement sector and would therefore be brought within the scheme in Part 3 of the Bill. We can confirm that financial institutions will not fall within Part 3 as they are not 'competent authorities' for the purpose of that Part. Rather, Part 2 is the relevant Part, together with the GDPR. Relatedly, paragraph 12 of Schedule 1 to the Bill make express provision for suspicious activity reports.

### Impact on journalism and other 'special purposes'

The Government is keen to preserve the exemptions for journalism and other 'special purposes' processing provided for in the 1998 Act. Lord Black of Brentwood and Viscount Colville of Culross both spoke eloquently as to the importance of this. We have already responded to their points in relation to clauses 164 and 165 of the Bill.

They also queried the impact of the right to rectification and the right to be forgotten on those processing personal data for journalistic purposes. As set out in paragraph 24 of Schedule 2 to the Bill, the controller may disapply a range of rights if they reasonably believe that the application of the right would be incompatible with the journalistic purpose for which the data is being processed. That is to be determined on a case-by-case basis. We continue to engage on this issue as we are determined to support high quality journalism.

### Law enforcement processing

Lord Stevenson of Balmacara picked up on the point that the Information Commissioner had raised in her briefing about the scope of clause 41(3) which restricts certain rights of data subjects under Part 3 of the Bill. The policy aim behind this provision is twofold. First, it enables police forces to refuse a subject access request where it relates to "relevant personal data" given that defendants in criminal proceedings already have access to such data through alternative routes, for example, in England and Wales under the disclosure provisions in the Criminal Procedure and Investigations Act 1996. Second, the provision reflects recital 20 of the Law Enforcement Directive which seeks to protect judicial independence.

### Intelligence services processing

Lord Lucas asked for clarification of provisions in Schedules 10 and 11 to the Bill which relate to intelligence services processing. Paragraph 4 of Schedule 10 replicates the existing provision in paragraph 5 of Schedule 3 to the 1998 Act. It allows for the processing of sensitive personal data by the intelligence services where the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject. Protection is provided by the data protection principles (in the case of Part 4, set out in clauses 83 to 89) including that the purpose of such processing must be specified, explicit and legitimate and data must not be processed in a manner that is incompatible with the purpose for which it is collected.

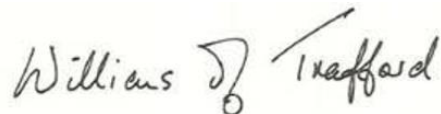
Paragraph 8 of Schedule 11 provides for an exemption from certain provisions in the Bill to the extent that the application of those provisions would be likely to prejudice the economic well-being of the UK. This provision is not creating a new purpose for which data can be processed. Rather, it reflects the fact that safeguarding the economic well-being of the UK is an existing statutory function of each of the intelligence services and provides the lawful basis for processing for that purpose. This will be relevant where the primary risk is to economic security, for example investigations into instability in parts of the world or unexpected crises which may undermine British markets and other economic interests.

We are copying this letter to all Peers who spoke in Tuesday's debate, Lord Clement-Jones and the Information Commissioner; we are also placing a copy in the House Library. If you would like to discuss these, or any further points, in more detail, please do not hesitate to get in touch.

Yours sincerely



**Lord Ashton of Hyde**



**Baroness Williams of Trafford**