Department for Digital, Culture Media & Sport

Lord Ashton of Hyde
Parliamentary Under Secretary of State
4th Floor
100 Parliament Street
London SW1A 2BQ

020 7211 6000

www.gov.uk/dcms

TO2017/07229/DC
13 November 2017

My Lords

Data Protection Bill: Day 2 of Committee Stage

It is once again my pleasure to write to you to follow up on a number of issues arising at Committee Stage of the Data Protection Bill.

Children and the internet

Baroness Jay of Paddington rightly highlighted that many of the issues we debated around, for example, the responsibility of social media companies, have a strong international flavour. The internet is a global network and many of our interventions will need to be international if there are to be effective.

We believe that the United Kingdom can lead the world in providing answers. The Government is already engaging with the leading tech companies and other like-minded democracies about rights and responsibilities online. Through the Digital Charter we will look to build consensus around rules for the digital economy. We are also in discussion with the next Presidencies of the G7 (Canada) and G20 (Argentina) about the importance of addressing these challenges. We recognise the complexity of this task and that this will be the beginning of a process, but it is a task which we believe is necessary and which we intend to lead.

Harmful content

Lord Alton raised the distressing issue of so-called 'suicide sites' – websites which attempt to promote, glorify or encourage the taking of one's own life. This is, of course, not an issue limited to the protection of minors, but rather one that has the potential to affect many of the most vulnerable people in our society. It is almost unthinkable that such sites would exist, and I thank the noble Lord for bringing the fact that they do to the attention of the Secretary of State and myself.

It is an offence in England and Wales to intentionally encourage or assist the suicide of another person. The person committing the offence need not know the other person or even be able to identify them, nor does the law require that a suicide in fact be attempted. I would therefore encourage anyone coming across such a site of the kind described to Lord Alton to report it to police. I will reflect further on whether there is more we can do as part of our broader internet safety work.

Equality of opportunity

Lord Lester asked whether the provision in paragraph 7 of Schedule 1, which allows processing of sensitive personal data for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment, constituted 'over legislation'. Having reflected on this, I can be unequivocal in setting out the Government's view that it does not. The Government firmly believes there is a need to reduce all forms of inequality described in the Equality Act 2010, including in relation to sexual orientation and religious and philosophical belief. Initiatives to identify or keep under review the existence of absence of equality of opportunity – for example, those undertaken by employers – are a key enabler in this space, regardless of which protected characteristic is being considered. This would be much more difficult without the inclusion in the Bill of paragraph 7 of Schedule 1.

I should add that, as paragraph 7(5) of Schedule 1 makes clear, data subjects will be able to require the controller to stop processing it for these purposes at any time. They also have access to the broader data subject rights concerning rectification and being forgotten.

Processing in relation to the prevention of bribery, terrorist financing and modern slavery

Lord Clement-Jones explained that Thomson Reuters carries out checks for financial institutions to identify customers and suppliers engaged in reprehensible activities like bribery, terrorist financing and modern slavery. Such checks necessitate the processing of sensitive personal data and criminal records data. As I explained during the debate, the Data Protection Act 1998 was amended to permit processing of such data without the consent of the data subject where it necessary to prevent crimes under certain UK laws, such as the Terrorism Act 2000 and the Proceeds of Crime Act 2002 and permits processing for anti-fraud purposes. The Bill replicates these provisions. While we are not yet convinced of the need to amend these provisions, I will be writing again to Thomson Reuters and others before the next stage of the Bill with a view to reaching a shared understanding of the impact of these provisions.

Biometrics

During the debate I committed to set out in more detail why the Government considers that the activities listed in amendment 66A are already permitted under Article 9.

As we discussed during the debate, most devices allow service users to use alternative methods of accessing the device, such as entering a password. When somebody uses biometric identification to access a computer or another service, that person would normally have made a conscious and freely made decision to use the verification

mechanism, which should satisfy the processing condition in Article 9(2)(a) on consent. The Government accepts that, under the GDPR, consent must be freely given, specific, informed and unambiguous and this may require some changes in the way current verification systems operate.

Where an employer had installed biometric verification as a means of allowing employees to enter their work premises, employees could be invited to consent to the use of the verification device. Alternatively, processing may be permitted for reasons of substantial public interest under Article 9(2(g) and Schedule 1 to the Bill – for example, on the grounds that it is necessary for ensuring the safety and security of employees. The concept of necessity is important here. Where there are less intrusive means of checking the identity of those entering the building these should be used instead. However, in cases where premises do need to be protected by a high level of security, reliance on Article 9(2)(g) may be appropriate.

Finally, the amendment considers the processing of sensitive personal data that is necessary "for internal research and development to improve a biometric identity verification and authentication mechanism". I should begin by saying that the concept of necessity is important here. Where 'internal research and development' can be adequately undertaken on the basis of artificial or non-identifiable biometric data, or data collected consensually from data subjects aware that it would be used for testing purposes, it can and should be.

In the event that it is genuinely necessary for a data controller to process data without consent for 'internal research and development', they should look to the processing condition relating to scientific research in Article 9(2)(j). As Recital 159 makes clear, the term ''scientific research'' is broad and covers activities including technological development and demonstration, fundamental research, applied research and privately funded research. Relevant safeguards are provided by Article 89(1), and include ensuring that technical and organisational measures, such as pseudonymisation, are in place to keep the data safe. These are supplemented by the safeguards in clause 18 of this Bill which prohibit research which causes substantial damage or distress or leads to decisions being taken about individual data subjects.

<u>Status of recitals</u>

Lord Kennedy suggested in debate that --

> "[The Minister], I and the House know that the recitals will not form part of British law [post Exit]…" (*Hansard,* vol 785, col 1647)

I apologise if I have inadvertently misled the noble Lord, but this is simply not correct. The EU (Withdrawal) Bill will convert the full text of direct EU instruments into UK law. This includes recitals, which will retain their status as an interpretative aid.

The noble Lord may have inferred the contrary because the recitals are not copied out in the applied GDPR. Let me put his mind at rest on this point. There is no need for the recitals to be copied out in this way, because clause 20(5) makes provision for UK courts to establish the meaning or effect of terms in the applied GDPR with reference to the meaning or effect of terms in the GDPR, including its meaning or effect in light of its recitals. I confess that it is not easy to navigate these provisions, but, as I have said before, we are looking here simply to bridge the relatively short period of time between the GDPR coming into force and the UK's exit from the EU.

I am copying this letter to the Secretary of State for Digital, Culture, Media and Sport, Baroness Williams of Trafford, Baroness Chisholm of Owlpen, the Minister for Digital and all Peers who spoke in Monday's debate and the Information Commissioner. I am 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.

Lord Ashton of Hyde
Parliamentary Under Secretary of State