



Department for
Digital, Culture
Media & Sport



Home Office

TO2017/07817/DC

24 November 2017

My Lords,

Data Protection Bill: Days 4 and 5 of Committee Stage

We write to you to follow up on a number of issues arising on days 4 and 5 of Committee Stage of the Data Protection Bill.

Clause 15 (power to make further exemptions etc by regulations)

Lord Stevenson thought it might be helpful if we put down in writing the Government's thinking in relation to the powers contained in clause 15.

Articles 6(3), 23(1), 85(2) and 89 of the GDPR provide derogations enabling Member States to make specific provision in domestic legislation, for example to restrict the application of the GDPR in certain limited circumstances, and subject to certain safeguards. They do not permit Member States to repeal, amend or revoke the GDPR itself. We have exercised these derogations in schedules 2 to 4 to the Bill.

All that clause 15 does is enable the Secretary of State to make further provision in relation to those same derogations. The scope of the powers in clause 15 is therefore limited by the scope of the derogations themselves. Accordingly, clause 15 no more permits the Secretary of State to amend, repeal or revoke the GDPR than Articles 6(3), 23(1), 85(2) or 89 do themselves. This is underlined by the words "altering the application" in clause 15 itself.

The Accreditation Regulations 2009

Lord Stevenson was right to say that, while the UK Accreditation Service (UKAS), is appointed as the UK's national accreditation body in a statutory instrument (2009 No. 3155), the substance of their role is set out in a directly applicable EU Regulation (No 765/2008). The EU (Withdrawal) Bill will convert that Regulation into domestic law at the point of exit.

GDPR application post-Brexit

On day 4 of Committee, Lord Stevenson remarked:

The implication from discussion on a previous set of amendments was that the requirements under the GDPR for extraterritorial application—so that when companies are not established in the EU, they need to have a representative here—will be dropped once we leave the EU... – *Hansard*, vol. 785, col. 2045

He may have inferred this from the non-extraterritorial application of the applied GDPR. If so, we apologise if we have inadvertently misled the noble Lord. We might refer him to the Government's previous response on this point:

Some people have suggested that the applied GDPR represents what the GDPR may come to look like once the UK leaves the EU. In some respects, this is a reasonable conclusion to draw. The applied GDPR anglicises the language and strips out irrelevant provision... However, in some respects, it is not the same as what future legislation will look like, including on the question of extraterritoriality. When we leave the EU, the powers in the EU withdrawal Bill will bring the GDPR into our domestic law, anglicised—as has been done to the applied GDPR—but also with other modifications that are dependent on the future negotiations with the EU. – *Hansard*, vol. 785, col. 1206

Requirements for a EU- (or, post-Exit, UK-) based representative, to which the noble Lord referred later on day 5 of Committee, fall into the same category as extraterritoriality.

The noble Lord also asked whether there was a case for tasking the Information Commissioner with ensuring the consistent enforcement of the provisions regarding data protection impact assessments within the UK. If the noble Lord means that the Information Commissioner should work to ensure these requirements are consistently applied by controllers across the UK, then we concur. The point that the Government was making was simply that the applied GDPR only extends to the UK, and other Member States will have different (and in some cases no) prescribed standards in relation to comparable processing activities. As a result, no inter-supervisory-authority consistency mechanism akin to that contained in the GDPR itself is appropriate for the applied GDPR.

As above, arrangements post-Exit may well be different to those set out in the applied GDPR. The UK is seeking a new, deep and special partnership that provides for ongoing regulatory cooperation between the EU and the UK on current and future data protection issues, building on the positive opportunity of a partnership between global leaders on data protection.

Public domain data

Baroness O'Neill asked about Amendment 153. Having checked her contribution in *Hansard*, it is possible her question was in fact directed at Lord Paddick. But it might nevertheless be helpful to clarify. The noble Lady talked about 'public domain' data 'not in the control of any data controller'. It is important to note that the concept of control is defined with reference to processing activities and not the underlying data (clause 5). One cannot process 'public domain' data and claim neither to be a controller nor know who the controller is.

Meaning of “defence purposes”

Baroness Hamwee expressed concern about the scope of the term “defence purposes” and questioned whether it would cover, for example, “records of the holiday leave taken by cleaners, secretaries and so on working in the Ministry of Defence” (Hansard, vol. 785, col. 2053). The term is indeed intended to be limited in both application and scope and will not encompass all processing activities conducted by the Ministry of Defence.

Only where a specific right or obligation is found to be incompatible with a specific processing activity being undertaken for defence purposes can that right or obligation be set aside. The Ministry of Defence will continue to process personal information relating to both military and civilian personnel in a secure and appropriate way, employing relevant safeguards and security in accordance with the principles of the applied GDPR. It is anticipated that standard HR processing functions, such as the recording of leave and management of pay and pension information will not be covered by the exemption.

The Government understands the need for the scope of the term to be defined more clearly, and accordingly we will provide further clarification in the explanatory notes to the Bill when they are re-issued on Commons Introduction.

Use of EU derived language

In speaking to a number of different amendments last Wednesday, Baroness Hamwee questioned the appropriateness of importing into the Bill some of the language used in the Law Enforcement Directive (LED). As explained in paragraph 59 of the Explanatory Notes to the Bill, and consistent with the transposition guidance adopted by the Coalition Government in April 2013 and applied since then, the approach we have taken in Part 3 is to copy-out the LED wherever possible. Deviating from this approach would itself risk creating legal uncertainty, not least because much of language used in Part 3 (for example the term “legitimate”) also appears in the directly applicable GDPR. If we were to depart from such language in Part 3, the courts would assume that Parliament intended that a different meaning should be ascribed to like provisions in the GDPR and Part 3 which adopted different terminology; this, however, is not our intention. Additionally the term “strictly necessary” already appears in UK law, for example in the Trafficking People for Exploitation Regulations 2013 so we are not breaking new ground in using the term in this context. Given this background, we hope Peers would agree that adopting the copy-out approach wherever possible is the right one in the context of the LED.

Archiving, etc

Lord Stevenson sought further clarification of the need for clause 39 (and paragraph 6 of Schedule 8), which applies to processing of personal data for law enforcement purposes where it is necessary for archiving, scientific, historical research or statistical purposes. Often, such processing will be anonymised so the data subject cannot be identified. However, on occasion it will be necessary to process personal data and this is envisaged by the LED (see Article 4(3)). UK law enforcement agencies advocate the concept of ‘evidence based policing’ which requires the use of best available evidence to inform and challenge policies, practices and decisions.

It is clearly in the public interest for this to continue and it will often require the review of historical data, and on occasion liaison with academic partners. There may also be instances in which data is specifically collected for archiving or for research by law enforcement agencies; an example of this would be to ascertain the developing approaches to tackling child abuse cases over several decades.

Periodic reviews of the need for the continued storage of personal data

Lord Stevenson also sought clarification of the expectation upon data controllers to take action following a period review of the need for the continued storage of personal data as envisaged by clause 37(2) (Hansard, vol. 785 col. 2062 and 2065).

Clause 37(1) requires the controller to process data for no longer than is necessary. If following a review of data carried out by a controller under clause 37(2), the controller concluded that it was no longer necessary to retain particular data; its continued storage would be in breach of the fifth data protection principle. Moreover, clause 35, which sets out the third principle, requires personal data processed for a law enforcement purposes to be “relevant”; if the continued storage of such data was found not to be necessary, the Government does not believe that the controller could reasonably argue that it was, nonetheless, still “relevant”. The Government is therefore of the view that the Bill as currently drafted provides sufficient safeguards to ensure the deletion of any data found not to be necessary.

Conditions for sensitive processing under Part 4: medical purposes

Finally, Baroness Hamwee probed why processing data for “medical purposes” was a condition for sensitive processing by the intelligence services under paragraph 7 of Schedule 10 to the Bill.

In his response, Lord Young explained that the medical purposes condition would be used for processing of medical data by medical professionals processing the services’ data. The example given was an intelligence services’ occupational health services carrying out fitness for work assessments and providing medical advice.

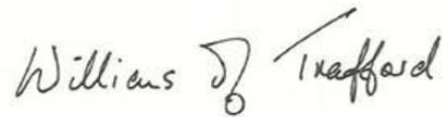
Baroness Hamwee suggested that this condition gave the intelligence services an advantage over employers in completely different fields. However, this is not the case. Paragraph 2 of Schedule 1 to the Bill provides for processing for “health or social care purposes” to be a condition for processing under the GDPR or applied GDPR. Sub-paragraph (2) of that paragraph lists, amongst other things, “the assessment of the working capacity of an employee” as consistent with these purposes.

We are copying this letter to Baroness Chisholm of Owlpen, the Minister for Digital, all Peers who spoke in the debate and the Information Commissioner. We will also place 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 with us.

Yours sincerely

Handwritten signature of Lord Ashton of Hyde in black ink.

Lord Ashton of Hyde

Handwritten signature of Baroness Williams of Trafford in black ink.

Baroness Williams of Trafford