UKCGC

The United Kingdom Caldicott Guardian Council

The Data Protection Bill

Summary

December 2017

Purpose

This document provides:

- a high-level overview of the Data Protection Bill, including details of the Parliamentary passage;
- key points of relevance around how health and care data might be affected.

Please note this document reflects a summary of the bill as of December 2017 and that for the latest updates regarding the Data Protection Bill please visit the Parliament UK website.

The Data Protection Bill

A bill to make provision for the regulation of the processing of information relating to individuals; to make provision in connection with the Information Commissioner's functions under certain regulations relating to information; to make provision for a direct marketing code of conduct; and for connected purposes.

Parliamentary passage

The Data Protection Bill was introduced to the House of Lords on 13 September 2017[1]. During second reading of the Bill on 10 October 2017, a wide-ranging discussion took place on issues including the reform of protections for the processing of general personal data, age verification and security.

The bill passed through its committee stage in the Lords during November and a new, amended version has been published. This briefing contains some information about some of the amendments that were made.

The bill will have the first two days of its report stage in the Lords on 11 and 12 December. It will have a further half day at this stage on 10 January, before passing to the 3rd reading in the Lords approximately a week later.

It is expected to be in the Commons by the end of January.

The advent of the GDPR into UK law in May 2018, means that the bill needs to pass before then in order to ensure the EU legislation is effectively interpreted within the UK context.

Overview

The Data Protection Bill proposes to:

- update UK data protection laws for the digital age where an ever increasing amount of data is being processed;
- empower people to take control of their data;
- support UK businesses and organisations through the change;
- ensure that the UK is prepared for the future after it has left the EU.

[1] https://services.parliament.uk/bills/2017-19/dataprotection.html

General data processing

The Government's aims for the bill in this area are to:

- implement the GDPR standards across all general data processing;
- provide clarity on the definitions used in the GDPR in the UK context;
- ensure that sensitive health, social care and education data can continue to be processed to ensure continued confidentiality in health and safeguarding situations can be maintained;
- provide appropriate restrictions to rights to access and delete data to allow certain processing currently undertaken to continue where there is a strong public policy justification, including for national security purposes;
- set the age from which parental consent is not needed to process data online at age 13.

Law enforcement processing

The Government's aims for the bill in this area are to:

- provide a bespoke regime for the processing of personal data by the police, prosecutors and other criminal justice agencies for law enforcement purposes;
- allow the unhindered flow of data internationally whilst providing safeguards to protect personal data.

National security processing

The Government's aim for the bill in this area is to:

- ensure that the laws governing the processing of personal data by the intelligence services remain up-to-date and in-line with modernised international standards, including appropriate safeguards with which the intelligence community can continue to tackle existing, new and emerging national security threats.

Regulation and enforcement

The Government's aims for the bill in this area are to:

- enact additional powers for the Information Commissioner, who will continue to regulate and enforce data protection laws;
- allow the Commissioner to levy higher administrative fines on data controllers and processors for the most serious data breaches, up to £17m (€20m) or 4% of global turnover for the most serious breaches;
- empower the Commissioner to bring criminal proceedings against offences where a data controller or processor alters records with intent to prevent disclosure following a subject access request.

How does this differ from the GDPR?

The Government intends the Bill to be a complete data protection system, so as well as governing general data covered by GDPR, it covers other general data, law enforcement data and national security data. Furthermore, the Bill exercises a number of modifications to the GDPR intended to make it work in UK in areas such as academic research, financial services and child protection.

Areas of particular relevance to the National Data Guardian

Engagement with stakeholders has highlighted three potential areas of interest to the NDG:

1. Section 162
2. Clause 15
3. Research concerns
4. Registries
5. Amendments 175-178.

Section 162

Section 162 outlines a new criminal offence that applies if an organisation knowingly or recklessly re-identifies information that is "de-identified" personal data, without the consent of the data controller responsible for de-identifying the data.

During debates about the bill in the Lords, concerns have been raised that security experts could be wrongly caught by this offence when undertaking testing of cyber security arrangements.

It is anticipated that the Government may introduce an amendment at report stage to clear that there would be a defence available to this offence where re-identification had occurred during legitimate activity to test security and where the ICO or the data controller had been alerted to this.

Clause 15

The BMA and others have raised concerns that clause 15 could give the Government an inappropriate procedure to change the law on how confidential health data are shared with very little scrutiny.

Clause 15 of the Data Protection Bill embeds a provision in Article 6 of the GDPR, which allows for member states to determine "*specific provisions to adapt the application of the rules*" of the GDPR for the lawful processing of data. Article 6 allows member states to determine their own "*specific requirements*" for when data are being processed (i) in compliance with a legal obligation, (ii) for the performance of a task in the public interest, or (iii) in the exercise of official authority.

The Bill does not set out these "*specific requirements*" on the face of the Bill. Instead clause 15 legislates that the UK will define its specific requirements for the lawful processing of data through *secondary legislation*. Such regulations will be made by the Secretary of State and affirmed by Parliament.

The BMA and others have raised concerns that clause 15 could, in effect, give the Government an inappropriate, fast-track procedure to change the law on how confidential health data are shared with very little scrutiny or oversight by Parliament or key stakeholders. The BMA argues that the law, as it stands, gives healthcare a special status of protection in the form of the common law duty of confidentiality which goes above and beyond the Data Protection Act (and the forthcoming GDPR). It believes that Clause 15 would allow for regulations to be laid that could override existing safeguards for confidentiality and, therefore, seriously undermine the trust-based relationship between a doctor and his or her patient.

The Lords' scrutiny select committee has said that the power is "*inappropriately wide*" and that the affirmative procedure for secondary legislation "*is not an adequate substitute for a Bill allowing Parliament fully to scrutinise proposed new exemptions to data obligations and rights*" and have recommended its removal from the Bill.[2]

An amendment 108A was put forward during the Committee stage in the Lords which would have said that "() Nothing in this section authorises the making of regulations which would enable a disclosure which contravenes the common law duty of medical confidentiality." However, this amendment was not accepted by the Government.

At the report stage in December the Government acknowledged concerns about the broad range of the powers and has introduced amendment 9 which would remove the previously proposed power of a Secretary of State to "omit" conditions and safeguards in Schedule 1.

Presenting this amendment, Baroness Chisholm of Owlpen said:[3]

"In its report, the committee raised concerns about the Henry VIII powers in Clauses 9(6), 33(6) and 84(3), which enable the Government to make regulations to "add to, vary or omit" the processing conditions and safeguards for sensitive data set out in Schedules 1, 8 and 10 respectively. Amendments 9, 90, and 99 respond to these concerns and narrow the regulation-making powers in these clauses. Amendment 9 removes the Government's power to omit processing conditions and safeguards in Schedule 1."

The committee also advised that the Government has introduced a new clause which would require consultation over any regulations made under clause 15 not only with the ICO but also with "such other persons" considered appropriate. He said that where this involved health data, this would include the NDG. We discussed that a similar commitment had been made when the Digital Economy Act was proceeding through Parliament.

Presenting this amendment, Baroness Chisholm of Owlpen said:[4]

"Amendment 166 reflects the concerns raised by noble Lords in Committee that regulations made under the Bill should be subject to consultation, not only with the Information Commissioner but also with consumer organisations and others who represent data subjects. Accordingly, we are including a requirement in Clause 169 that when the Secretary of State makes regulations under the Bill, she must consult "such other persons" as she considers appropriate. This will apply to all regulations save for those listed in new subsection (2A). We have also tabled consequential Amendments 126, 131, 135 and 138 to remove the equivalent requirement from Clauses 133(1), 142(9), 148(6) and 152(3) to avoid unnecessary duplication in the light of the new general requirement in Clause 169."

Stakeholders concerned about this clause intend to continue to press this issue.

[2]Delegated Powers and Regulatory Reform Committee, '6th Report of Session 2017-19: The Data Protection Bill' (25/10/17), Clauses 15 to 11: https://publications.parliament.uk/pa/ld201719/ldselect/lddelreg/29/2906.htm - _idTextAnchor004

[3] https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/18066en.pdf - Column 1465

[4] https://hansard.parliament.uk/lords/2017-12-11/debates/6E9F6986-18AA-45D5-B51F-33F597CFC4A0/DataProtectionBill(HL – Column 1466)

Research concerns

There have been some concerns that the legislation would leave some medical research without a sure legal basis, however, it looks like the Government has acknowledged these and that a solution will be found.

Wellcome Trust, the MRC, Cancer Research UK, the AMRC, the Sanger Institute, the Academy of Medical Sciences and the ESRC among the stakeholders raised concerns about the potential for the bill as drafted to have a negative impact on medical research.

They have concerns that the bill does not provide a clear legal basis for universities to be able to conduct research using personal data. There are three options, but as drafted it appears that none of these are sufficient:

a) *Consent:* It would be difficult for researchers to comply fully with stricter GDPR requirements for consent, particularly where the details of future research are not yet known.

b) *Legitimate interests*: Universities are considered 'public authorities' as defined in the Bill (Clause 6) and GDPR rules out public authorities relying on *'Legitimate interests'* as a legal basis for processing.

c) *Public interests*: Clause 7 of the Bill appears to restricts 'public interests' to a concept concerned with public and judicial administration and there remains a lack of clarity over whether this would cover university-based research.

In the Committee stage in the Lords[5], Lord Patel moved two clauses to address this which would have made clear in the bill that 'public interests' that explicitly includes research purposes.

In responding, Lord Ashton said that Clause 7 is deliberately designed to be indicative and non-exhaustive and committed to make this clearer in the Explanatory Notes. He said that:

"it is difficult to expand Clause 7 to cover every scenario where personal data has been processed in the public interest…It is absolutely not the Government's intention to impede pioneering medical research, which can have tangible benefits for society as a whole. The noble Lord's suggestion of disapplying the safeguards if the research project has been approved by a relevant medical ethics review body is certainly worthy of further consideration. I am happy to work with him and other noble Lords to explore it further in the coming weeks. On that basis, I invite the noble Lord to withdraw his amendments."

The amendment was withdrawn at this stage and at the report stage amendments 72 to 77 were tabled to address this.

In presenting the amendment Lord Ashton said:[6]

"Government Amendments 72 to 77 are the products of detailed discussion with the noble Lord, Lord Patel, the noble Baroness, Lady Manningham-Buller, and representatives of the Wellcome Trust. I thank them very much for those constructive and helpful discussions. In Committee we discussed the operation of the safeguards in Clause 18 and the potentially damaging impact they would have on pioneering medical research. As I explained at the time, it was never the Government's intention to

[5] https://hansard.parliament.uk/Lords/2017-10-30/debates/0A5454BD-E626-4268-A594-688A38F5806C/DataProtectionBill(HL) (Column 1252ff)

[6] https://hansard.parliament.uk/lords/2017-12-11/debates/6E9F6986-18AA-45D5-B51F-33F597CFC4A0/DataProtectionBill(HL) - Column 1478

undermine such important work, so it is with great pleasure that I table these amendments today.

"Noble Lords will recall that the greatest concern stemmed from the safeguard in what is currently Clause 18(2)(a). That paragraph was designed to prevent researchers using personal data to make measures and decisions in respect of particular data subjects but, as the noble Lord explained, there are certain types of medical research where this is inevitable. In the context of a clinical trial, for example, a data subject might willingly agree to participate, but in the course of the trial researchers might need to make decisions about whether the treatment should continue or stop, with respect to some or all data subjects. Government Amendment 77 addresses this concern by making it clear that the safeguard is automatically met where processing is necessary for the purposes of approved medical research. Approved medical research is defined in the new clause and includes, for example, research approved by an ethics committee established by the Health Research Authority or relevant NHS body. Importantly, the new clause also contains an order-making power so that the definition of approved research can be kept up to date."

Registries/historic consents

Baroness Neville-Jones has raised with ministers concerns of charities supporting individuals with genetic conditions about registries which they maintain. The concerns that they have raised is that the historic consents do not meet GDPR standards. At the report stage in December, the Government Committed to examining this.

We discussed the fact that similar issues have been considered by the NDG and others in the health and care system and some of the applicable principles in the NDG Review and Caldicott Principles. The official said the DDCMS may wish to engage with the NDG on this matter.

In speaking about this matter at the report stage, Lord Ashton said:[7]

"My noble friend Lady Neville-Jones explained in Committee that Unique plays a hugely important role in providing advice and support to sufferers of rare chromosomal disorders and their carers. Some of these charities have large databases dating back many years, so we understand their desire to maintain these when the GDPR comes into force without necessarily obtaining fresh consent to GDPR standards for each data subject included on the database. When families are providing support to their loved ones, some of whom may need round-the-clock care, filling in a new consent form may not be high on their agenda.

"However, they may still value the support and services that patient support groups provide and would be concerned if they were removed from the charities' databases. If charities such as Unique had to stop processing or delete records because consent could not be obtained, they worry that this would impede the work they do to put patients and their families in touch with others suffering from rare genetic conditions, help clinicians to deliver diagnoses and facilitate research projects. We recognise that this could be particularly damaging when there is barely any knowledge of the condition other than what they may hold on their database.

"Let me be clear: if there is a grey area in the Bill that puts this work at risk, the Government are fully prepared to amend it. Legislating in this area is not straightforward

[7] https://hansard.parliament.uk/lords/2017-12-11/debates/6E9F6986-18AA-45D5-B51F-33F597CFC4A0/DataProtectionBill(HL) – Column 1478

and I am keen that the policy and legal teams in the department are able to continue with the constructive discussions they have been having with Unique and the UK Genetic Alliance to ensure that the legislation adequately covers the specific processing activities they are concerned about, while providing adequate safeguards for data subjects. I assure noble Lords that we will use our best endeavors to work on this legislative solution as quickly as possible. If it is not ready by Third Reading, and I am afraid I cannot promise it will be, the Government will endeavor to introduce any necessary provisions at the next possible amending stage of the Bill. I will of course ensure that my noble friend gets the credit she deserves for her persistent efforts on this subject when that time comes."

Amendments 175-178

At the Report stage in the Lords, the Government introduced new clauses 175-178 which allows the Secretary of State to create a Framework for Data Processing by Government. Concerns have been raised by MedConfidential that this would allow a Secretary of State to create rules for his or her Department's processing of data which would take it outside the purview of the ICO.

It is expected that the Government will be publishing a Statement of Intent giving detail about the intention of the framework and its potential scope before the bill progress to the House of Commons.

Further links

Data Protection Bill (HL Bill 66)

Data Protection Bill Impact Assessment

Data Protection Bill Overview

Data Protection Bill: General Processing

Data Protection Bill: Law Enforcement Processing

Data Protection Bill: National Security Processing

Data Protection Bill: Information Commissioner and Enforcement