House of Commons - Debate Briefing

All-Party Parliamentary Group on Data Analytics

Briefing ahead of second reading of the Data Protection Bill, and the effects of Brexit on GDPR

Thursday 1st March, 2018

About the All-Party Parliamentary Group on Data Analytics (APGDA)

The All-Party Parliamentary Group on Data Analytics is a cross-party group chaired by Daniel Zeichner MP to connect Parliament with business, academia and civil society to promote better policy making on big data and data analytics.

There are three pillars to the group.

1. What can be done to help UK business prosper aid investment decisions and define the boundaries of competition
2. To inform and empower the public on the collection and use of personal data, so they are willing participants in the new age
3. To develop a world class education division to deliver a skills base to give the UK a leading role in the worldwide use and exploitation of data

The APPG on Data Analytics facilitates effective, productive communication and exchange between Parliament, Government, and the public, private and third sectors. To achieve this, the group conducts a wide range of activities, including a programme of parliamentary meetings and in-depth parliamentary and policy monitoring. Our officers also ask questions in Parliament on data analytics.

The APGDA is run by Policy Connect, the cross-party think tank which seeks to successfully deliver new policy ideas through research, evidence, political meetings and sector engagement. For more information – **please visit the APGDA website**.

Recommendations and Methodology

This briefing was prepared following two Parliamentary roundtables held in January 2018. The discussion was led by APGDA Chair, Daniel Zeichner MP, and vice-chair Stephen Timms MP, and brought together leading figures from across the data analytics sector, including businesses, civil liberty advocates, and academics. Amongst the groups attending the roundtables were:

- Experian
- Information Comissioners Office
- Privacy International
- SAS Software
- Cicero
- Brunel University
- Direct Marketing Association
- ARM
- The ACCA

A presentation was also given by the Information Commissioner's Office, the UK's national data protection authority. ICO is a statutory body sponsored by the Department of Digital, Culture, Media and Sport.

The APGDA makes the following **broad recommendations** for the second reading, and committee stages, of the Data Protection Bill. These recommendations take into account the view of a wide-range of APGDA members and are set out with the view of improving the legal framework to be established by the landscape in a way that improves the regulation of personal data, as well as ensuring that the United Kingdom will remain at the forefront of innovation and the digital economy.

1. To ensure the independence of the **Information Commissioner's Office** from Government in-line with the regulations of GDPR, Members should consider the impact of Clause 188(5) on the ability of the ICO to carry out regulatory duties free from potential overreach by the relevant Secretary of State. This clause states:
    a. In determining a question arising in connection with the carrying out of any of the Commissioner's functions, the Commissioner must take into account a provision of a document issued under section 186(3) if—
        i. (a) the question relates to a time when the provision was in force, and
        ii. (b) the provision appears to the Commissioner to be relevant to the question[1]
2. To consider the **future role** that could be played by ICO in the relation to the growing debate over the impact of data in automation, with particular reference to the Centre for Data Ethics as announced in 2017's Autumn Budget.
3. To maintain a level of **competitiveness** between Government bodies and the private sector with regard to attracting the best talent.
4. To clarify the scope and remit of the **Code of Conduct** for age appropriate design, especially were pertaining to **children's data**.
5. To explicitly set out the exceptions with which GDPR will apply with regard to the purposes of "**national security and defence**" as set out in Clause 26.

These policy recommendations have bet set out with a view to amending the Bill whilst understanding the need for a new legal and regulatory framework for how Government and the private sector handle personal data. It is the view of the APGDA that the Data Protection Bill is a necessary piece of legislation that must be adopted to create a system fit for current and future challenges.

However, the recommendations detailed above serve to achieve the following:

- Guaranteeing the **full independence** of the Information Commissioner's Office, ensuring confidence in the UK's regulatory system from businesses, private individuals, and foreign agencies
- Allows for ICO and other bodies to influence future debates and legislation for challenges in **emerging technologies**
- Ensures that outstanding questions regarding **civil liberties** are addressed and are legally enforceable by the Judiciary

[1] Parliament, **Data Protection Bill [HL]**, (Retrieved: 12th January 2018) p. 108

The Data Protection Bill

The Data Protection Bill is part of a commitment by the Government expressed in the 2017 Conservative Manifesto to repeal and replace the United Kingdom's existing data protection laws. This follows significant advances in technology and the digital economy since the passing of the Data Protection Act 1998. In particular, the Bill aims to accommodate demands for individuals to have more control over personal data submitted online, and to set out a regulatory framework following the UK's withdrawal from the European Union and the Digital Single Market.

The Department for Digital, Culture, Media and Sport sets out the aims of the Bill as follows[2]:

- Replace the Data Protection Act 1998 with a new law that provides a comprehensive and modern framework for data protection in the UK, with stronger sanctions for malpractice.
- Set new standards for protecting general data, in accordance with the GDPR, give people more control over use of their data, and provide new rights to move or delete personal data.
- Preserve existing tailored exemptions that have worked well in the Data Protection Act, carrying them over to the new law to ensure that UK businesses and organisations can continue to support world leading research, financial services, journalism and legal services.
- Provide a bespoke framework tailored to the needs of our criminal justice agencies and national security organisations, including the intelligence agencies, to protect the rights of victims, witnesses and suspects while ensuring we can tackle the changing nature of the global threats the UK faces.

The Bill also seeks to formally apply the standards of the forthcoming General Data Protection Regulation (GDPR) into statue law. Although GDPR is implemented as part of EU-wide legislation, the act ensures that the standards will remain convergent with those of the European Union following Brexit in March 2019, allowing for a degree of continuity for businesses after Brexit. A recent study by the data services company, W8data, found that the UK is one of the leading EU nations for preparedness for GDPR.

Of the ten largest nations in Europe ranked by gross domestic product, only 29 percent of UK organisations claim to be 'unprepared' for the introduction of GDPR in May 2018, compared with 48 percent in Germany, and 54 percent in France[3]. However, the Government has warned that awareness of GDPR differs across sectors of the economy, with the construction and manufacturing organisations especially low-ranked[4].

Ahead of the second reading of the Data Protection Bill in the House of Commons, the All-Party Parliamentary Group on Data Analytics (APGDA) held two roundtables regarding online identity, GDPR and the Data Protection Bill. These events brought together parliamentarians, academics, businesses, and experts in privacy and transparency. This briefing is therefore intended to:

- Provide an overview of GDPR and the Data Protection Bill
- Highlight issues arising from the legislation, as noted by APGDA members and other sources

[2] HM Government, **Data Protection Bill: Overview**, (Retrieved: 24th January, 2018)
[3] Infosecurity Magazine, **UK 'Most Well-Prepared' European Nation for GDPR**, (Retrieved: 26th January, 2018)
[4] HM Government. **Digital and Culture Secretary urges businesses and charities to prepare for stronger data protection laws**, (24th January, 2018)

- Note legislative recommendations made by APGDA members

This briefing sets out to explain the current status of the Data Protection Bill, as well as APGDA recommendations for how Parliamentarians may seek to amend the legislation. This is connected to the key priorities of the APPG to:

- Preserve and protect data rights, and to safeguard the civil liberties of individuals from excessive state and commercial intrusion
- To ensure that Britain remains at the forefront of digital technology and innovation
- Ensuring any regulatory divergence from Brexit does not hinder the operations of British organisations and businesses

Key issues

The most recent estimates by DCMS place the value of the digital sector to the British economy at £118.4bn[5]. The digital sector represents the largest component of the areas that DCMS gathers statistics on, responsible for 14.2 percent of total UK service exports in 2015. It is clear that maintaining a digital economy that is open, innovative and decentralised is essential to maintaining Britain's competitive advantage in the sector. As currently written, the Data Protection Bill does not pose a serious threat to this. However, any overreach by the Government to overly regulate the sector could have serious repercussions for this key economic sector. This risk is independent of the wider questions posed by Brexit.

According to DCMS[6], the main elements of the Bill are:

General data processing

- 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

- 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
- 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

[5] HM Government, **DCMS Sectors Economic Estimates 2017**, (retrieved 26th January, 2018)
[6] HM Government, **Data Protection Bill: Overview**, (Retrieved: 24th January, 2018)

Regulation and enforcement

- 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

The Data Protection Bill was introduced by Lord Ashton of Hyde – the Parliamentary Undersecretary of State – to the House of Lords on 13th September 2017. It passed its third reading in on 17th January 2018 and was subsequently given its first reading in the House of Commons the following day. During the Lords debates – a number of amendments were made to the Bill. Most significantly, Clause 188 sets out a new framework by which government Departments can process and share data[7]. The APGDA concurs with the Information Commissioner's Office (ICO) that the clauses are currently set out lack clarity and as currently written could lead to a state of regulatory confusion, especially if codes of practice clash with those already given statuary status as part of the Digital Economy Act, 2017.

In particular, Clause 188(5) compels the Commissioner to take into account the provisions of the framework according to the Secretary of State. This could lead to serious limits – even theoretically – being placed on the independence of the ICO, contravening Article 52 of GDPR[8].

The APGDA also supports the introduction of new points in Clauses 171, "Re-identification of de-identified personal data", following a recent report by the Guardian newspaper that previous drafts of the bill would have inadvertently criminalised legitimate, authorised research into the effectiveness of encryption by organisations[9]. Whilst seemingly a minor point, this highlights the importance of close scrutiny of legislation that deals with such a complex legal area as data protection and cybersecurity.

The Digital Economy, Data Protection, and Brexit

Regardless of rhetoric in other areas, policy makers in both the United Kingdom and the rest of the EU have expressed a willingness to maintain level of regulatory alignment with other European states with regard to data protection. This is especially clear with regard to sharing of information on security and policing across the EU. On numerous occasions, most recently at the World Economic Forum in Davos, the Prime Minister has made it clear that she feels that the United Kingdom should remain at the forefront of global cybersecurity and data sharing efforts by security services[10].

[7] House of Commons, **Data Protection Bill [HL]**, (18th January, 2018), p. 108
[8] PrivazyPlan, **Article 52 EU GDPR "Independence"**, (retrieved 26th January, 2018)
[9] The Guardian, **Data protection bill amended to protect security researchers**, (9th January, 2018)
[10] BBC, **Davos: Theresa May Warns Tech Firms Over Terror Content**, (25th January, 2018)

Additionally, Giovanni Buttarelli, the EU's Data Protection Supervisor, has said that the UK remains a "potential strategic partner" to the EU in future[11], although he has cautioned that this is dependent on a successful conclusion to the forthcoming Brexit negotiations[12].

With this in mind, Lords Select Committee on the European Union noted in July 2017 that maintaining a common regulatory framework that it was "struck by the lack of detail in the Government's assurances thus far"[13] whilst also warning of the risks of a "cliff-edge" in the event of a lack of a transitional deal being established ahead of March 2019[14].

Additionally, the Bill pledges to incorporate GDPR and the Police and Criminal Justice Directive into British Law following Brexit. However, the Government has also proposed withdrawal from the Charter of Fundamental Rights in areas of this 'retained legislation'. This could potentially lead to a legal environment where the UK's data protection laws diverge from the pan-EU system – leading to challenges in adopting a common regulatory framework. Whilst this matter forms part of the wider legislative framework by which Government approaches Brexit, it is matter that may also be discussed within during the Committee stage of the Data Protection Bill.

Contact Details

For more information about the work of the APGDA, Policy Connect and other issues, please contact:

Dr George Dibb
Head of Industry, Technology and Innovation:
george.dibb@policyconnect.org.uk
0207 202 8586

Jack Tindale
Manager, Design and Innovation
jack.tindale@policyconnect.org.uk
0207 202 8588

[11] Computer Weekly, **UK likely to remain strategic EU data protection partner**, (26th January, 2018)
[12] European Commission, **Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection**, (9th January, 2018)
[13] House of Lords, Brexit: the EU data protection package, (18th July, 2017) p. 35
[14] *Ibid*