

techUK briefing on the Data Protection Bill
House of Commons Second Reading –
Monday 5 March 2018

Jeremy Lilley
Policy Manager
+44 (0) 7545 204 098
Jeremy.lilley@techuk.org

10 St Bride Street
London
EC4A 4AD

T 020 7331 2000
F 020 7331 2040
www.techuk.org

About techUK

techUK is the industry voice of the UK tech sector, representing more than 950 companies who collectively employ over 800,000 people, about half of all tech jobs in the UK. These companies range from innovative start-ups to leading FTSE 100 companies. The majority of our members are small and medium sized businesses.

This briefing is a summary of the key issues in the Data Protection Bill that affect the UK's technology sector, ahead of the Bill's Second Reading in the House of Commons on Monday 5 March 2018. The briefing will set out the key issues set for debate. The UK is recognised as a world leader in both data protection and data innovation. This Bill should help ensure this remains the case.

Key Messages

- The **Data Protection Bill is welcomed by the tech sector** as a way of ensuring the UK's data protection laws are fit for the digital age. Ensuring that the public can trust their data is handled safely is important for everyone.
- **The passage of this Bill is crucial and time-sensitive.**
- The Government is right to use the Data Protection Bill to help put the UK in the best position possible to **agree a mutual adequacy agreement with the EU** to allow the continued free flow of data post-Brexit.

The Data Protection Bill Should Remain Narrow

The Data Protection Bill should remain narrow and have a clear focus on legislating for the derogations under GDPR

- techUK believes this Bill is necessary and that all parties should support its passage to ensure the UK correctly implements GDPR and relevant derogations.
- This is **time sensitive**, as the derogations must be in place by 25 May 2018 when GDPR takes effect. The Law Enforcement Directive parts of the Bill must be in place by 6 May 2018.
- Given its importance and time sensitivity, this Bill should not be seen as an opportunity for wider discussions around the use of information.
- **A narrow Bill will also put the UK in the best position possible to secure a successful Brexit.**

The Data Protection Bill updates UK data protection for the digital age

- The **Government's Data Protection Bill is welcomed by the UK tech industry.**
- The Bill will significantly increase the control that citizens have over how their personal information is used.
- As goods and services are increasingly digitised, data protection laws should seek to ensure people can continue to access these goods and services whilst holding companies accountable for protecting user data.
- Tech companies take data protection incredibly seriously, as it is key to the trusted relationship between companies and customers, and support smart and effective data protection laws. The implementation of GDPR will help ensure that people can trust that their data will be handled safely.

Data-driven businesses will bring substantial economic benefits but only if a culture of data trust and confidence is established

- The UK's Data Economy is expected to be worth **£241 billion by 2020, creating an additional 157,000 new jobs.**
- Data-driven innovation stands to provide significant benefits across the economy and society.
- This ranges from the increased personalisation of goods and services, cost efficiencies for businesses and the improvement of public services.
- However, those benefits will only be realised if a **culture of data trust and confidence** is established in the UK, where citizens are brought along the data journey.
- The Data Protection Bill is an important part of establishing that culture of data trust and confidence.

Data Protection is a core issue across the entire economy

- This is not only a serious issue for the tech industry. **Organisations of every size and sector, both public and private, are increasingly using personal data** to deliver services.
- The definition of personal data is being expanded and so more types of data will be caught by this Bill.

The Data Protection Bill is necessary to secure a good Brexit deal

Maintaining the frictionless free flow of data between the UK and EU post-Brexit must be a priority. The best way to achieve this is through an adequacy agreement with the EU. Implementing the GDPR will be a positive step in the right direction.

- **Data is a vital enabler of not just the UK digital sector but the overall UK economy and society.**
 - As the economy becomes increasingly digitised all sectors will rely on data flows.
 - Data flows underpin finance, retail, manufacturing, automotive and health sectors.
 - For example, the latest Ford GT has more lines of code in it than a 787 Dreamliner, showing the increased digitisation of cars.
 - The Government have confirmed that 'over 70% of trade in services are enabled by data flows, meaning that data protection is critical to international trade'
 - The UK accounts for 11.5 per cent of global data flows, 75 per cent of which are with the EU.
- **Digitally intensive industries account for 16% of Gross Value Added (GVA), 24% of total UK exports, and three million jobs** (techUK, ['The UK Digital Sectors After Brexit'](#)).
 - The sector is **growing 32% faster than the national average** (Tech Nation 2017).
 - **96% of sector output and 81% of sector exports are spread across services activities** (techUK, ['The UK Digital Sectors After Brexit'](#)).

Once the UK leaves the EU the automatic ability to transfer data between the UK and EU27 will be lost.

- **The Government have set out their position on data flows post-Brexit and are seeking a bespoke model.**
 - Rt Hon Matt Hancock MP, Minister for Digital, had previously [committed to 'unhindered data flows'](#) and has highlighted the importance of maintaining the frictionless free flow of data.
 - The Government's Position Paper envisages a bespoke model for data flows post-Brexit, **'building on the current adequacy processes'**.
 - Within that bespoke model the Government is seeking a continued role for the UK ICO on the European Data Protection Board.
 - While the aims and objectives of the Government's position are positive, **more detail is needed on how it intends to proceed with establishing that agreement.**
 - There are a number of issues that remain unresolved by the Government's position paper which will need to be discussed with the European Commission.

- **Securing an adequacy agreement offers the most robust and least burdensome way of retaining data flows with the EU.**
 - **Adequacy is most suitable mechanism for SMEs**, who will find transferring data difficult without adequacy. The utmost of efforts must be made to have this in place by the day we leave the EU to avoid a cliff-edge.
 - Achieving adequacy will require the UK's post-Brexit data protection framework to be 'essentially equivalent' to the EU's. **Therefore, implementing GDPR in order to have the same framework as the EU27 will be an important step.** This does not preclude the UK from utilising the available derogations within the GDPR.
 - An adequacy assessment by the European Commission will take into consideration all areas of domestic law pertaining to data protection, not just those covered by EU competency i.e. including national surveillance laws.
 - The House of Lords EU Home Affairs Sub-Committee agreed with techUK, [following an inquiry](#), that adequacy is the best method to ensure data can continue to flow between the UK and EU post-Brexit.
 - The House of Lords report recognised that transitional arrangements may be required to avoid a cliff-edge.
 - We now need clarity on how the Government intends to secure 'unhindered data flows'. This should be through an adequacy agreement.
- **Alternative mechanisms available under the Data Protection Directive and the incoming GDPR are unstable and ill-suited for the majority of UK businesses, particularly SMEs.**

Post-Brexit the UK Government will also have to determine whether other third countries are adequate

- **With the UK implementing the GDPR, it will also implement requirements to determine the adequacy of third countries before allowing the free flow of personal data to those third countries. This will include the EU.**
 - As part of the Brexit process the UK Government will have to establish processes to monitor data transfers outside of the UK. This will include having a system in place to consider the adequacy of third countries.
 - techUK has been clear that mutual adequacy agreements are needed between the UK and EU to allow the continuous free flow of data. This will involve the UK determining whether the EU is adequate.
 - Processes will also be required to determine whether the UK will recognise existing EU adequacy decisions with countries such as Canada and New Zealand. techUK believes this should be done in a timely manner.
 - The UK will also need to replicate the EU-US Privacy Shield to ensure continued data flows with the US.
 - Work on the UK's adequacy processes must begin now, and the Government should set out the work it is conducting in this area.

Annex – EU General Data Protection Regulation – The Basics

- The EU General Data Protection Regulation (GDPR) is the most significant reform to data protection laws in over twenty years.
- It updates and replaces the Data Protection Directive 1995 (implemented in the UK as the Data Protection Act 1998).
- It took almost five years of negotiation between the European Commission, European Parliament and EU Member States.
- The EU Regulation, which has direct effect, was adopted on 14 April 2016 with an implementation date of 25 May 2018.
- The reforms put citizens at the heart of data protection with the principles of Transparency and Accountability at the forefront of the new rules. Citizens and consumers will have much greater control over who has their personal information and what happens to it.
- The GDPR will apply throughout the EU and beyond due to the extra-territorial reach of the regulation. This means that wherever a European resident's data is being processed, no matter where the processing takes place, the GDPR rules will apply.
- The definition of personal data is being expanded under the GDPR. The new definition is: *“any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”*
- This wider definition means that more types of data will be within the scope of the Data Protection Bill affecting organisations of every size and sector.
- The GDPR provides data subjects with additional controls and rights over their data including:
 - Right to be forgotten
 - Right to rectification
 - Right to data portability
 - Right of access
- There are also considerable new responsibilities on organisations that process personal data including:
 - Joint liability of data processors and data controllers.
 - Transparency
 - Accountability
 - Significant fines for non-compliance of up to 20 million euros (£17 million) or 4 per cent of Global Annual Turnover.
- For more information on how GDPR will impact technology companies please see this blog: <https://www.techuk.org/insights/news/item/6842-how-will-new-eu-data-rules-impact-my-tech-business>