techUK briefing on the Data Protection Bill

House of Lords Report Stage – Week Commencing Monday 11 December 2017

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 Report Stage in the House of Lords, starting on 11 December 2017. The Briefing will set out the key issues and amendments 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 Government has accepted the need to provide reassurance that the UK is committed to a right to data protection. techUK welcomes their amendment and hopes that Peers will accept it.
- The Government's amendment on age appropriate design is a sensible compromise to address concerns expressed at Committee Stage about processing children's data while maintaining UK compliance with GDPR.
- A new criminal offence against re-identifying de-identified data ***should focus on the use case which inspired the offence and should not prevent legal processing of de-identified data under the GDPR.***

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.
- Given its importance and time sensitivity, this Bill should not be seen as an opportunity for wider discussions around online safety.
- A **narrow Bill will also put the UK in the best position possible to secure a successful Brexit.**

Key Amendments at Report Stage

Proposed Amendments on a Fundamental Right to Protection of Personal Data

- There are two amendments on a fundamental right to data protection, one tabled by the Labour Party and one tabled by the Government.
- Following discussion at Committee Stage, the Government have accepted the need to include a form of wording which provides a suitable level of assurance that the principles of Article 8 of the EU Charter of Fundamental Rights
- The Government's amendment should achieve the aim of ensuring there is no perception that the UK will draw back its commitment to data protection as it leaves the EU and techUK believe this amendment should be supported.
- The amendment is particularly welcome in light of important further discussions taking place on the Charter as a whole as part of the passage of the EU (Withdrawal) Bill through the House of Commons.

Amendment on Minimum standards for age appropriate design

- Following discussions at Committee Stage on whether there should be a minimum standard of age appropriate design for services used by children, the Government has reached a compromise with Baroness Kidron and has put forward a joint amendment.
- This amendment would require the ICO to produce a Code of Practice on age appropriate design, which should be consulted on and be delivered within 18 months of the Bill becoming law.
- **This is a sensible alternative** as this Code could then complement the work between Government and Industry to tackle concerns around child online safety, such as through the Internet Safety Strategy, which are more appropriate vehicles to address these concerns. It also provides a more flexible approach to tackling these issues of concern.
- **Crucially important, this approach would avoid the potentially negative impact on GDPR implementation and UK-EU adequacy agreements.**

Proposed Amendment: "Personal data ethics advisory board and ethics code of practice"

It is right to consider how to approach ethical issues relating to data use however techUK does not believe the Data Protection Bill, which is a technical Bill to update data protection laws to give citizens the rights and controls they need, is the right place to address the important issue of data ethics. There is also already considerable amount of work already going on in this area.

The Data Protection Bill is not the right place to address data ethics:

- We are about to enter a new era where machine learning and AI are at the heart of future technological driven innovation ethical questions are likely to arise as to the use and processing of personal data. It is entirely right and proper that those ethical issues are identified and considered.
- Many of the questions being raised about the ethical use of and impact on personal data from machine learning and AI are in fact data protection questions, rather than ethics, and can already be addressed by existing data protection laws and the incoming GDPR and Data Protection Bill.
- The ICO has stated the GDPR introduces "stricter rules" for personal data that are "no different for big data, AI and machine learning" The GDPR has been designed in such a way as to maintain privacy rights and standards for citizens as technological advances continue. The GDPR provides individuals with the relevant tools and rights to protect their personal information and gives them control over how that information is used
- The GDPR also ensures the UK will have a regulator, in the form of the ICO, that can address the questions being raised today. Creating an additional body at this stage could confuse the role of the ICO, which is recognised as a world leading Data Protection Authority, well-placed to address concerns around the processing of personal data.

However, it is right that Government takes the issue of data ethics seriously. That is why techUK supports the significant amount of work already being undertaken in this area. This work, in particular the creation of a new Centre for Data Ethics and Innovation, means that the amendment is unnecessary. Work includes:

- In the 2017 Autumn Budget, the Government announced a new 'Centre for Data Ethics and Innovation' with funding of £9 million. This fulfilled a Conservative Party Election Manifesto commitment. Given this announcement, this amendment seems unnecessary. techUK looks forward to continued engagement with Government on the new Centre for Data Ethics and Innovation.
- A recent report by the Royal Society and British Academy, of which techUK was a leading member of the working group which made a number of recommendations, including the creation of a data stewardship body, which are being further considered.
- The creation of a Convention on Data Ethics by The Nuffield Foundation which is expected to begin its work in 2018.
- A Digital Ethics Summit organised by techUK on 13 December 2017 to consider the ethical data issues raised by the emergence of AI technologies.

techUK would encourage this amendment to be withdrawn. Given the various activities already underway in this area, it risks duplicating work and cutting across already established mechanisms. It would also be inappropriate to legislate for a new body which could confuse the role and important work of the ICO.

Other Areas in the Data Protection Bill

Age of Consent – Section 8

- The **tech sector supports the Government's intention to set the age of consent at 13.**
- Digital and interactive services are of societal and developmental benefits to teens, and a crucial element of **developing digital literacy**. To require parental consent for all users under 16 years old would prevent individuals benefiting from services which offer significant social and educational benefits to them.
- Using these services help children and young people **develop the skills, critical thinking, knowledge, resilience and support** they need to navigate the online world safely as an adult.
- Many information services develop **content specifically for young people, including educational materials.** Preventing children from accessing this content could cause significant disruption. Setting the age above 13 would incentivise children to lie about their age and make it impossible for companies to appropriately target specific content to them. This could ultimately lead to making children's online experience less safe.
- Evidence from Ofcom shows that a majority of parents believe that the **benefits of their child's technology use outweighs potential harms**, and has a positive impact on their future, career and life skills.
- **Setting the age at 13 would also align with global practices**. Much of this international best practice stems from the US Children's Online Privacy Protection Act (COPPA) and child safety experts, digital policy experts, anti-bullying organisations, youth organisations and educational groups, among others, all support retaining a lower age. Given the significant amount of cross-border digital activity, harmonisation should be an objective.

Re-identification of de-identified personal data – Section 162

- The Data Protection Bill introduces a new criminal offence for the re-identification of de-identified data. **This is not an element of the GDPR.**
- The Bill's Explanatory Notes cite a narrow use case of medical care and research, however as drafted the offence could capture a large number of other, legitimate, activities.
- In some situations, re-identification of pseudonymous data may be legitimate and necessary such as when testing a security system to ensure it is effective.
- There are **other aspects of law which prevent individuals from using personal data for reasons other than which it was collected**, such as identify theft and fraud.
- Within the GDPR itself if personal data is used for a purpose for which it was not originally collected or processed, the data controller would have no legal basis to process and therefore be in breach of GDPR and liable to the fines.
- Similarly, the GDPR did not envisage a hierarchy of legal basis for processing and so setting consent as the gold standard is at odds with the GDPR.
- As drafted this offence would go further than the GDPR, gold plating the regulation in UK law. **It should be amended to allow the re-identification of de-identified data to the extent to which it is lawful to do so under GDPR, and narrowed to focus on the specific use cases which inspired the offence.**

Right to claim compensation - Section 159

- Section 159 is intended to identify the circumstances under which consumers could claim compensation. These provisions are contained within Article 82 of the GDPR.
- The Bill reflects the current Data Protection Act but extends grounds for a claim beyond financial loss and distress to include "other adverse effects".
- **This new terminology is open to broad and highly subjective interpretation** and could invite vexatious claims. We would recommend that section 159 is limited to financial loss and distress in line with the current Data Protection Act.

Scope - Section 186

- The GDPR establishes the extra-territorial scope of the regulation. Section 186 replicates this for areas where GDPR applies.
- However, the 'Applied GDPR' does not retain this extra territorial reach, applying only to controllers and processors established in the United Kingdom.
- The Bill's explanatory notes state that the GDPR and Applied GDPR will be merged into a single framework post-Brexit but does not say how this will happen. Specifically, there is no mention about whether the extra-territorial reach of the GDPR will be retained.
- It is **important that there is legal clarity as how this is intended to apply after the UK exits the EU.** If the extra-territorial reach is not maintained there would be a significant disincentive for controllers and processors to establish themselves in the UK.
- Government has made clear it will seek an enhanced role for the ICO alongside other Data Protection Authorities (DPAs) as part of its paper "The exchange and protection of personal data: A future partnership paper".
- **Clarity is needed on how the ICO will continue to work with other DPAs post-Brexit,** so that there is an understanding on how cross-border complaints involving UK consumers will be progressed. In particular information is needed as to how the ICO will interact with the 'one-stop-shop' approach of the GDPR.

Protection of free expression - Part 5 of the Bill

- Part 5 of the Bill outlines the GDPR exemptions in Article 85(2) for reasons of freedom of expression and information. Government has decided to limit the exemptions to media publishers which are already protected under s32 of the Data Protection Act.
- There is a growing use of data protection law by influential claimant lawyers to bypass the stricter test of libel and other laws to secure the removal of content from online services and suppress legitimate speech, which may be in the public interest.
- Section 32 of the Data Protection Act provides a defence to the media publisher, but not online intermediaries on whose platforms publisher content may have been shared. We believe that freedom of expression and the public interest are best safeguarded by closing the gap in the law which is being widely exploited by litigants and extending this defence to online intermediaries.

Annex A - Background to the Data Protection Bill

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.

Annex B - 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 though 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.**

Annex C – 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 identify 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