techUK briefing on the Data Protection Bill

House of Lords Second Reading

10 October 2017

Jeremy Lilley
Programme 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 Lords on 10 October 2017. The UK is recognised as a world leader in both data protection and data innovation. This Bill should help ensure this remains the case and helps to develop a post-Brexit Global Britain.

Executive Summary

- 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.
- ***All major parties agreed to implement the EU General Data Protection Regulation (GDPR)*** at the 2017 General Election. This ***Bill should have the narrow focus*** of legislating for GDPR derogations along with necessary legislation for data processing not covered by EU competencies.
- This Bill is **time sensitive.** It must be **in place before May 2018** in order to ensure that UK meets its obligation to implement GDPR. The ***Bill should be seen through the prism of Brexit***, full implementation of GDPR is necessary to ensure that the UK is in the best possible position to secure a ***mutual adequacy agreement with the EU to allow the continued free flow of data post-Brexit.***
- The ***Government is right to set the age of consent at 13***. This will allow young people to reap the societal and educational benefits of online activity, as well as helping them to develop the digital skills which are now fundamental for young people to have. A higher age threshold risks excluding people from these tools. The policy goal of protecting young people's data is accomplished through safeguards within the GDPR designed to prevent harm to young people, such as potential harm from automated decision making.
- The Data Protection Bill ***must allow data to be processed for research purposes***, as currently allowed by the Data Protection Act 1998.
- The ***Information Commissioner's Office must be well-resourced*** so it can effectively undertake the important work it has to do in developing compliance guidance for new data protection rules.
- A new criminal offence against re-identifying de-identified data ***should not prevent important security research,*** which would make systems less secure, not more.
- The Data Protection Bill must operate in conjunction with the EU (Withdrawal) Bill. It is important that the right to protection of personal data under the European Charter of Fundamental Rights is protected in order to give the public the overall right to recourse over personal data protection.

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 use these 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.

Implementing the General Data Protection Regulation

All the major political parties committed at the 2017 General Election to implement GDPR

- The Government, and other political parties, committed to implementing the EU General Data Protection Regulation despite the vote to leave the EU.
- GDPR comes into direct effect in the UK on 25 May 2018 and will be brought into domestic law through the European Union (Withdrawal) Bill.
- However the GDPR also contains a number of 'derogations' whereby Member States can adapt the GDPR. The Data Protection Bill offers the UK Government the opportunity to legislate for those derogations.
- All EU countries will apply these derogations in different ways in order to ensure that GDPR implementation fits with their national standards.
- More information on the GDPR is available in the annex.

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, which is also implemented via the Data Protection Bill, must be implemented into national law by 6 May 2018 which provides a deadline for the passage of the Data Protection Bill.
- 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.**

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.**

What the Bill does – GDPR Derogations

Unlike many EU Regulations the GDPR sets out a number of derogations, whereby Member States can alter the regulation. techUK welcomes the Government's decision to replicate as far as possible the exemptions found within the Data Protection Act 1998. The key derogations contained in the Bill include but not limited to:

- **Age of consent – Section 8**
  - The **tech sector supports the Government's intention to set the age of consent at 13.**
  - Online services are of societal and developmental benefits to teens. 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.
  - This is **not just about social media sites**, the age of consent covers everything from education websites to TV players. Too high a restriction risks cutting young people off from necessary resources.
  - 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.
  - An ability to take part in digital life is a crucial element of **developing digital literacy.** There are a number of programmes which have been developed in partnership through industry and civil society, which 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.
  - As the world becomes increasingly digital it will be important for people of all ages to have fundamental digital skills. Allowing young people to interact with online services from a young age will help them develop those skills.
  - 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 a retaining a lower age. Given the significant amount of cross-border digital activity, harmonisation should be an objective.
  - **Section 187 relating to Children in Scotland** also needs clarification as there could be confusion if harmonisation in the UK is not achieved. Section 187 suggests Children in Scotland can consent at the age of 12.

- **Processing criminal data – Section 9 (5) and Parts 1, 2 and 3 of Schedule 1**
  - The Government is proposing to enable organisations other than those vested with official authority to process data relating to criminal convictions and it is right to do so.
  - Ensuring organisations are able to process this data is important and it is vital that there are the legal basis to do so, such as those found in the current Data Protection Act.

- This is important for a variety of reasons, such as ensuring organisations can run criminal checks on potential employees and carry out corporate due diligence.
- **In Schedule 1, part 3, section 22**, the Bill states that criminal convictions data can be processed if the data subject has given their consent. **To ensure consistency with the GDPR this should be 'explicit consent'**.
- This may also be important from an anti-corruption perspective; some legislation requires controllers to have effective procedures to reduce the risks of corruption. Included within those procedures are carrying out effective due diligence to understand partnerships (e.g. vendor relationships; hiring consultants; sponsorships) that may give rise to corruption. For higher risk partnerships, this may involve reviewing security and criminal convictions data.

- **Automated decision making – Section 13**
  - The GDPR states that individuals will have the right not to be subject to automated decision making where this produces 'legal effects or similarly significant affects' apart from in a narrow set of circumstances.
  - **However, the Bill refers to a 'significant decision' as a decision producing 'legal effects' or 'significantly affects the data subject', removing the word 'similarly'**. The purpose of the GDPR is to not limit safeguards against automated decision making to legal effects but also effects that are similar to legal effects. The word 'similarly' is therefore important to ensure that non-legal effects resulting from automated decision making are akin to legal effects. **'Similarly' should be re-inserted into section 13's definition of a 'significant decision' when talking about significant effects.**
  - The **safeguards already contained in the GDPR are sufficient** to ensure that citizens are protected against automated decision making which affects them significantly or legally.
  - Adding further provisions around automated decision making would add unnecessary burden to businesses who are already planning for the current text of the GDPR across Europe, without providing additional meaningful privacy protections to UK data subjects. Sections 13(6) and (7) should be deleted.

- **Research and Development – Section 14 (1)(f) and Part 6 of Schedule 2**
  - The Data Protection Act 1998 makes provision for exemptions to the Act for R&D where suitable safeguards are in place.
  - The GDPR limits this to 'scientific and historical' research, however Member States are able to legislate for additional exemptions where safeguards are in place.
  - techUK believes that the Data Protection Bill's **provisions for 'scientific and historical research' should be broadened out, with the same provisions of Section 33 of the Data Protection Act 1998.**
  - The definition of 'scientific and historical research' also needs clarification. For example it is not clear whether this would include computer science engineering research.
  - Paragraph 4 of Part 1 of Schedule 1 adds a requirement for the processing of special categories of data necessary for scientific or historical research purposes. According to the Data Protection Bill such processing must be in the public interest, which goes beyond the GDPR. techUK strongly suggests the deletion of this additional requirement which constitutes a potential barrier to innovation.

- **ICO resourcing – Section 132**
  - Each Member State must appoint a National Data Protection Authority, which in the UK is the Information Commissioner's Office.

- The GDPR ends notification fees from data controllers to fund the work of the Information Commissioner's Office.
- The Data Protection Bill has established a system which would allow the ICO to collect fees from data controllers to fund its work, however more detail is needed on how this will operate in practice.
- The **ICO is an incredibly important regulator and a world-leader in its field, and must be funded appropriately**
- The Information Commissioner herself has stated that it will need additional resources to oversee the implementation of GDPR and developing associated guidance. The Government must ensure that the ICO has sufficient resources to carry out its important work.
- techUK believes that the implementation of GDPR must come hand in hand with greater resources for the ICO.
- However, the funding of the ICO should not be based on fines. Such funding would undermine the impartiality of the ICO when assessing fines against companies. The ICO should always remain in a position to assess organisations' compliance with the law from a neutral and objective perspective rather than being driven by potential gains of levying fines.

- **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 is not further defined in the explanatory notes.
  - **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.

- **Representation of data subjects – Section 173**
  - Section 173 utilises of the provisions in Article 80(1) of the GDPR which allows a data subject to authorise a representative to exercise certain rights on their behalf.
  - We note that some stakeholders continue to call on Government to also make use of Article 80(2) of the GDPR to allow a representative body to file a complaint independent of a data subject's mandate.
  - **We believe that Section 173 provides a sufficiently robust route to recourse for consumers and that this does not require the addition of the additional option set out in Article 80(2) of the GDPR.** This would, in our view, undermine the link between a claim and measurable harm to specific consumers, and could lead to vexatious claims being brought which would be a burden on the ICO's resources without yielding privacy benefits for UK consumers.

- **Scope - Section 186**
  - The GDPR establishes the scope of the regulation. Section 186 replicates this and states that the Bill extends to any entity offering goods and services to, or monitoring the behaviour of, UK consumers.
  - It is **important that there is legal clarity as how this is intended to apply after the UK exits the EU.** Government has, for example, 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.

- **Powers of entry and Inspection – Schedule 15**
  - Schedule 15 makes provisions for powers of entry and inspection
  - The Data Protection Bill should ensure that before gaining access to the premises the following conditions are met:
    - (1) advanced warning in writing announcing the specific purpose of the visit,
    - (2) permit a legal representative to be present;
    - (3) right to refuse access if these two conditions are not met;
    - (4) right of the controller/processor to mark documents business confidential or mark as non-responsive/irrelevant to the ICO's inquiry.

Applied GDPR – Chapter 3, Part 2 and Schedule 6

Clarity is needed about how the 'Applied GDPR' will work post-Brexit

- The EU GDPR only applies to areas of law within EU competency. The Data Protection Bill applies the GDPR provisions, with some amendments, to areas of law not covered by EU competency.
- The GDPR will be automatically brought into UK law through the European Union (Withdrawal) Bill.
- Once the UK leaves the EU no area of UK law will be within EU competency and so is not clear whether the GDPR, or the Applied GDPR, will be the sole UK data protection law.
- The Bill's explanatory notes suggest that once the UK leaves the EU the provisions of the applied GDPR (i.e. the application of GDPR to those areas not covered by EU law), and the actual GDPR will be merged, however does not state how this will be done. **Clarity is needed on how the GDPR and the Applied GDPR will interact post-Brexit and what will form the basis of a sole UK Data Protection Law**.

- Some amendments within the Applied GDPR are necessary for areas not covered by EU law i.e. references to other Member States or EU Institutions.
- However other areas amend GDPR quite significantly. For example the extra-territorial provisions of the GDPR are removed from the applied GDPR, representing a key difference.

New Criminal Offence

A new criminal offence should not prevent important security research

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 and has been added by the UK Government.**
- It is **not clear why the Government have introduced this new offence**. Its purpose is not clearly demonstrated although the explanatory notes suggest it is targeted at medical data.
- Introducing a new offence suggests that re-identifying personal data from de-identified data is possible. This goes against the principles of anonymised information.
- 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.
- ***At a minimum* research and security should be added as defences against this offence as important security research should not be prevented by this new offence.**
- Clarity is also needed on what constitutes 're-identification' as this is not clear.

The Data Protection Bill does offer an opportunity for the UK to maintain a commitment to Article 8 of the Charter of Fundamental Rights post-Brexit

- Clause 5(4) of the European Union (Withdrawal) Bill makes clear that the Charter of Fundamental Rights ('the Charter') will not become part of UK law as part of the replication process. techUK is concerned by this measure as it relates to Article 8 of the Charter, the right to Protection of Personal Data.
- **Article 8 underpins much of EU data protection law, including the GDPR,** and is crucial to the legal frameworks which allow for the free flow of data across European borders.
- techUK is concerned that, without this right being clearly replicated in UK law, Clause 5 of the Withdrawal Bill could be an impediment to negotiations between the UK and the EU on the need to secure an 'adequacy' agreement to allow the free flow of data post-Brexit.
- **techUK would therefore like to see a clear commitment from Government to Article 8 of the Charter retaining a position in UK domestic law**, or for its function to be replicated elsewhere on the statute book.
- It would therefore be appropriate for the Data Protection Bill to include a fundamental right to the protection of personal data, should the Government maintain its position on withdrawing from the Charter of Fundamental Rights as part of the Withdrawal Bill.

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 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