techUK position paper on India Data Protection Bill

September 2018

10 St Bride Street
London
EC4A 4AD

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

techUK | Representing the future

Contacts:
Jeremy Lilley | Policy Manager | Data Protection and Digital Single Market
T 07545204098
E jeremy.lilley@techuk.org

About techUK

techUK represents the companies and technologies that are defining today the world that we will live in tomorrow. More than 950 companies are members of techUK. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium-sized businesses.

Introduction

This position paper sets out techUK's views on the India Data Protection Bill 2018. The development of data protection framework within India is of significant interest to tech companies operating in the UK. India is an important trading partner for the UK and access to the Indian market is an important consideration for UK businesses with total UK-India bilateral trade worth £15.4 billion in 2016.[1]

In an increasingly digital and interconnected world, data and trade go hand in hand. The way in which personal data is to be treated and protected in India is therefore important to trading relations between UK and Indian businesses both in the tech sector and across the entire economy.

In general, techUK welcomes India's Draft Data Protection Bill 2018. It is a significant step forward in the development of data protection law in India. A large number of the Bill's provisions mirror that of the EU's General Data Protection Regulation (GDPR), which took effect on 25 May 2018. This is a positive development given the global nature of data protection. The global reach of GDPR means that many businesses across the world are already complying with GDPR and therefore alignment in more countries is beneficial. Indian legislation that meets the standards set by GDPR is also likely to be a key factor in the success of any attempt for India as a whole, or in the first instance, the Indian IT industry, to secure adequacy status with the EU. Adequacy status would significantly reduce barriers to trade between the EU, India and the UK.

However, there are some concerns with certain elements of the Bill, as set out below:

1. Data localisation requirements

The data localisation requirements within the Bill are arguably the most concerning element of the India Data Protection Bill. Their inclusion mirrors a disappointing trend of increasing data localisation requirements around the world. techUK urges India not to require a copy of all personal data to be stored on servers only in India as well as not mandate that critical data is only be processed on servers in India. techUK suggests these requirements should be removed from the Bill.

[1] https://www.ons.gov.uk/businessindustryandtrade/internationaltrade/articles/whodoestheuktradewith/2017-02-21

Data localisation does not assist with data protection in any way and instead causes significant operational disruption and increases the costs of doing business. Additionally, requiring data to only be located locally can compromise the security of personal data.

Where there is a cross-border data transfer system in place for personal data not classified as critical by the Central Government, techUK would suggest that India looks to international mechanisms which facilitate cross-border data transfers. For example, the Bill references Standard Contractual Clauses or Intra-group schemes approved by the Authority. India may well wish to look to the EU's set of Standard Contractual Clauses and Binding Corporate Rules as a basis to operate from in this regard. Alternatively, India may wish to consider how it may interact with the APEC Cross-Border Privacy Rules system.

On top of the restrictions already set out for data transfers, the Bill also refers to gaining the data principals' consent for a data transfer even where the data transfer has already satisfied requirements set out in the act. If the data transfer has satisfied those requirements (specifically Section 41 (1)(a) and (b)), additional consent should not be necessary.

2. Definitions

Generally, the definitions used in the Bill are acceptable and understandable. However, in certain cases further consideration is needed. In particular, the definitions of personal data and sensitive personal data should be revisited. Personal data should be defined as data that the fiduciary or processor is reasonably likely to have and use as the means to identify the principal – rather than any data that is capable of reidentification. The definition of sensitive personal data is too broad, and the types of data listed in the Bill covers data which is processed regularly. For example, by including passwords in the definition of sensitive personal data, additional and separate consent would be required by the fiduciary every time a data principal creates a new password. As a matter of fact, what is protected by password may be sensitive, but the password by itself is not sensitive personal data. It would be best for the law to be principles-based and not specific to technology like password. As a matter of fact, password is a particular technology and is increasingly being replaced by multi-factor authentication, token and biometrics, etc.

Additionally, the Bill contains a provision allowing the Authority to specify any type of data it deems appropriate as sensitive personal data via subordinate legislation. This would create significant uncertainty and data fiduciaries should not be expected to operate in a landscape where the rules can be changed at any point of time. There must be ample clarity within the principal legislation itself. The broad definition of sensitive personal data combined with the limited legal bases for processing sensitive personal data is concerning. The definition should be narrowed, and the legal bases extended.

3. Legal Basis of Processing

To avoid any confusion, the processing of "sensitive personal data" should be explicitly permitted as lawful where necessary for the purpose of complying with legal obligations applicable to the data fiduciary. In addition, reasonable purposes related to activities such as "prevention and detection of any unlawful activity including fraud"; "network and information security"; "credit scoring" and "processing of publicly available personal data" currently enlisted under Section 17 (2) should be allowed as default reasonable grounds per se rather than requiring any discretion or determination by the Data Protection Authority. Reasonable purposes for data processing should also be extended also to third parties, similarly to the legitimate interest legal basis provided under Article 6(1)(f) of the GDPR.

4. Sub-Processing

The proposal to allow the engagement of a sub-processor by a data processor only with the prior authorisation of the data fiduciary as provided in Section 37 (2) is neither necessary nor desirable or pragmatic. It would be preferable to have a parallel here again with the GDPR. Accordingly, the data processor should be able to obtain prior general consent of the data fiduciary, with an obligation to inform the latter before engaging a new sub-processor. This would provide the requisite flexibility to the data processor while offering reasonable opportunity for the data fiduciary to object, paving the path to resolution by way of mutual discussions and negotiations.

5. Powers of the Authority

In several Sections of the Draft Bill certain actions, definitions, time limits etc are left to the discretion of the Authority. Further clarity is needed on the face of the Bill so that businesses are able to fully understand, and comply, with the new rules. It is not fair or appropriate for key elements of this legislation to be amended by the Authority as this significantly increases the risk to businesses operating in India. Examples of this include but are not limited to: types of sensitive personal data; information to be included on a notice; time period in which fiduciary must comply with principals' requests; transparency requirements and information to be included in data audits. This flexibility for the Authority to re-define parts of the Bill should be removed and the provisions clarified within the Bill itself.

6. Age Verification

The Bill requires data fiduciaries to implement age verification processes to ensure the personal data of children is processed appropriately. However, many services are not aimed at children and therefore should not be expected to implement age verification systems. Doing so goes against data minimisation requirements in that a new database of sensitive personal data is being created by the fiduciary for no specific purpose. Those services not aimed at children should be exempt from this requirement.

7. Data Breach Notification

It is essential that data breach notification rules be risk-based, speedy and effective in mitigating the impact and harm rather than over-burdening the DPA with numerous instances irrespective of the extent of harm. Accordingly, first and foremost, Section 32 (1) should be revised as suggested below:

"The data fiduciary shall notify the Authority of any personal data breach relating to any personal data processed by the data fiduciary where such breach is likely to cause significant risk of impact or harm to the affected data principals."

However, for the transparency, accountability and breach notification measures discussed earlier to be effective, data fiduciaries need to be able to detect breaches in a timely manner. Accordingly, we suggest setting out guidelines for data fiduciaries and data processors on the context-relevant basic security requirements that they must put in place to help them protect personal data and detect breaches (e.g. if an organisation is collecting passwords, it must be subject to a certain minimum level of encryption).

A breach need not be communicated to data principals if appropriate, reasonable, adequate and proportional technical and organisational protection measures were in place at the time of the incident (e.g. encrypted data), so that the breach is unlikely to result in a significant risk of harm to the data principals.

8. Data Protection Impact Assessment – Data Auditor

There is a provision within the Bill to allow the Authority to determine whether an external Data Auditor is needed to carry out a Data Protection Impact Assessment. This would create significant costs for businesses and could make it less likely for businesses to launch products in India, giving consumers less access to technological advances.

9. Offences

techUK suggests that establishing criminal offences under the Draft Bill is inappropriate, as it risks is making natural persons liable for criminal offences performed in the official capacity of the legal person that employs them. Instead, the extant criminal law should be applied in case of mala fide actions with criminal intent.

Conclusion

techUK hopes these comments are helpful in the continued development of the Data Protection Bill and stands ready to assist further.