UK INDIA
BUSINESS COUNCIL

THE BUSINESS CASE FOR INDIA'S PERSONAL DATA PROTECTION BILL

GROUNDED IN EXTENSIVE INTERACTIONS WITH GOVERNMENT AND BUSINESS ACROSS THE UK-INDIA CORRIDOR, THE UKIBC HAS PREPARED THIS BRIEFING NOTE TO FACILITATE CONSULTATION ON THE GOVERNMENT OF INDIA'S DRAFT PERSONAL DATA PROTECTION BILL 2018 AND THE PROMISING FUTURE OF THE UK-INDIA TECH PARTNERSHIP.

MAY 2019

WHAT IS INDIA'S DRAFT PERSONAL DATA PROTECTION BILL?

India's Ministry of Electronics and Information Technology (MeitY) published in 2018 a draft Bill proposing a systematic, country-wide approach to protecting, collecting, processing, and transferring personal data in India.

The Bill proposes a 'quasi-consent, quasi-access' framework where in order to process a person's personal data you must have their informed consent. Once consent is given, an individual's ability to review, access, or edit their data is narrowly defined to prevent bias and confusion.

The Bill also proposes an overarching Data Protection Authority (DPA) much like the UK Information Commissioner's Office. The DPA would hold investigative, corrective, and advisory powers and will further be able to define categories of 'sensitive' data subject to more stringent localisation. As it stands, the Bill's data localisation provision appears to require those processing personal data to retain a copy in India. Only data classified as 'critical' will have to be both stored and processed in India.

UK business welcomes the the Bill as a necessary and positive step toward adopting intuitive, transparent, and fair data protection. The UK and India enjoy immense AI complementarities including our high ethical standards, economic ambition, alignment of expertise, enabling Government's, outward-looking AI strategy, innovative infrastructure and investment, and end-to-end positioning.

It is our belief that, subject to further consultation set out in this briefing note, an innovation-friendly Bill could unlock an immense partnership between the UK and India capable of delivering the Fourth Industrial Revolution.

WHAT ARE THE IMPLICATIONS OF THE BILL FOR BUSINESS?

A BETTER WAY TO ACCESS AND PROCESS DATA

Provisions on confirmation, access, breaches, and automated processing are potentially a significant improvement over the GDPR.

Once initial consent has been secured to automatically process personal data, it is costly and inefficient to reverse this if consent is withdrawn or the right to be forgotten enacted. The Bill recognises that this also risks unnecessarily introducing human bias and error into complex algorithms needed to clean, process, and translate data into AI outcomes. Keeping individual access to a high-level summary of their data use under the Bill effectively addresses these concerns and makes India an easier place to process data.

The GDPR requires the principal to be informed of all and any data breaches concerning them by the fiduciary. This risks spreading fear and misplaced confusion. The Bill however, ensures that the DPA, rather than the fiduciary, informs the principal, and only if direct harm has been caused. This is a sensible balance between maximising opportunity and minimising misuse.

INTUITIVE DATA LOCALISATION

Data transfer is the lifeblood of innovation, which, if compromised, could have ramifications for India's AI ambitions.

MietY has proposed localising data into three 'buckets'. The first bucket (sensitive personal and national security data) would be subject to hard localisation and cannot be transferred out of India. The second (personal and commercial data) will be subject to mirroring where a copy of the original data must exist on server in India. A third bucket of non sensitive data will not be subject to localisation.

Any level of localisation will require significant investment in data storage infrastructure in order to enforce a provision designed to boost India's domestic data centre industry. With reassurance and clarity, limited localisation can balance national security, individual privacy, and the transfer of data across borders vital for delivering India's international data processing ambitions.

If adopted, this provision needs to be sector and State-agnostic applying to all personal data systematically everywhere in India equally. Different requirements across sectors, States, and as well as by 'bucket', will make it difficult to enforce, regulate, and improve the ease of doing business.

A POWERFUL STATE EXECUTIVE

Both the 'lawfulness of processing' and the 'exemptions' provisions of the Bill are unique for large liberal nations as they allow Government to access personal data in the interest of national security without significant safeguards. The GDPR has similar exemptions, however, it has checks and balances mitigating potential misuse which the Bill does not. Adopting these forms of checks and balances can reassure citizens as to the proper access and use of their data by Governments.

AN INDEPENDENT DATA PROTECTION AUTHORITY

Ensuring a strong and independent DPA that is tech-savvy, fairly funded, and works with business will be critical to checking the State's power, engendering trust, and ensuring the continued relevance of data regulation.

In practice, the DPA interprets guidelines for which data requires consent or is exempt. This includes whether Government can see sensitive biometric, health, sexual orientation, and financial information.

To maintain trust, the DPA therefore needs to be truly independent and tech-savvy. However, the Bill gives Government significant influence over the DPA's Board Members proposed by a Select Committee.

Effective data governance also means building close relationships with data practitioners and sufficient structural flexibility enabling enforcement to adapt with innovation. Only governance embedded in the very methods AI uses, and the people who create them, will be future-proof, sustainable, and enforceable.

The DPA outlined in the Bill however, has the responsibilities of a regulator and enforcer. This raises the possibility of structural conflicts of interest unless carefully demarcated as in EU Member State DPAs. Given that the DPA is to be funded through fines, this also means perfect compliance would significantly reduce DPA income and enforcement capacity, providing mis-incentive in regards to penalty provisions.

Though there is currently no precedent for separating regulatory and enforcement responsibilities within existing Indian regulators, which are often funded through fines, establishing a new DPA gives the opportunity to introduce international best-practice.

DATA PROTECTION THAT DELIVERS FOR INDIA AND BUSINESS

In light of business needs, international best practice, and India's own ambitions, we make nine recommendations to minimise data misuse and maximise India's unique data opportunity.

1 DEFINE WHAT HARM JUSTIFIES NOTIFICATION

When harm to an individual determines if they are notified of a data breach, strong assurance and clear guidelines are needed to ensure the notification procedure is fair and accountable.

2 EFFICIENT DISPUTE RESOLUTION

Resource and expertise are necessary to deal effectively with data disputes through tribunal and adjudication procedures. Investment needs to be made into fostering data skills to ensure cases are heard fairly and quickly by qualified professionals and trust in the system upheld.

3 CLEAR, LIMITED, AND INTUITIVE DATA LOCALISATION

Free flow of data is integral to delivering innovation and India's AI ambitions. As such, businesses need explicit reassurance that extensive localisation only applies to sensitive data on an individual's identity or national security. A 'three bucket' approach to localisation will need clear, limited, and intuitive parameters that is sector-agnostic and applies to the data system as a whole including enforcement across States. A 'sector-bucket' regulatory matrix creates barriers to data transfer and business adaptation, whilst intuitive guidelines engender trust from businesses and individuals alike. These should be regulated by the DPA within the parameters set out in legislation.

4 SUPPORT INFRASTRUCTURE FOR LOCALISATION

Increasingly data storage infrastructure makes borders hard to distinguish in data. Businesses need to know what data formats will fulfil localisation provisions and where this requires significant development in architecture and infrastructure, the Government should commit funding and collaboration to deliver this.

5 MOVE EXEMPTION POWERS TO THE LEGISLATIVE

The 'exemption' provision concentrates significant powers in the executive who could initiate and review surveillance without a court order, any form of third-party review, or notifying the principal. This power should be moved, in line with other trusted data protection regimes, to the hands of the Legislative.

6 SEPARATE THE REGULATOR FROM THE ENFORCER

Pioneer international best practice through a clear and comprehensive separation of regulatory and enforcement powers either within a single DPA or across two separate regulatory and enforcement authorities to avoid potential conflicts of interest.

7 A FAIRLY FUNDED REGULATOR

Funding the regulator through consistent, and protected, levies on the organisations it directly oversees will allow sustainable operational capacity independent of enforcement and penalties. This avoids regulation based on budgetary needs.

8 A TRULY INDEPENDENT REGULATOR

To maintain trust, appointments to the DPA governing board should be recommended by a truly independent committee based on tech savviness and experience without Government influence.

9 A TECH-SAVVY AND SUSTAINABLE REGULATOR

To regulate at the pace of innovation, the Data Protection Authority needs strong communication with the technology practitioners themselves. This means clear and permanent dialogue with both business stakeholders and foreign regulators. Both domestic and foreign business should be consulted to ensure the most innovation-oriented and future-proof outcome.

UK INDIA
BUSINESS COUNCIL

WHO ARE THE UK INDIA BUSINESS COUNCIL?

The UKIBC is a non-profit, membership-lead, Government-backed organisation supporting business, trade, and investment in the UK-India corridor. We have a close working relationship with Ministries and Departments across Indian and UK Governments supporting business success.

This briefing note is the first in a series based on the in-depth report representing the voice of business on India's data protection and the future of the UK-India Tech Partnership published by UKIBC in March 2019. For information about our digital advocacy and wider work visit www.ukibc.com or get in touch with our Digital Sector Manager, Meghna Misra-Elder at meghna.misra-elder@ukibc.com

GET IN TOUCH

UK INDIA BUSINESS COUNCIL LONDON
15th Floor, Citibase, Millbank Tower
21-24 Millbank London SW1P 4QP
enquiries@ukibc.com
Tel: +44 (0)20 7592 3040

UK INDIA BUSINESS CENTRE MUMBAI
Trade Centre G/F & 1st Floor,
Bandra East,
Mumbai,
Maharashtra 400051
enquiriesindia@ukibc.com

UK INDIA BUSINESS CENTRE BANGALORE
Concorde Towers, UB City,
1 Vittal Mallya Road, Level 14 & 15,
Bengaluru, Karnataka 560001
enquiriesindia@ukibc.com
Tel: +91 (0) 806 7590 319

UK INDIA BUSINESS CENTRE GURGAON
WeWork DLF Forum, Cyber City,
Phase III, Sector 24,
Gurugram Haryana – 122002
enquiriesindia@ukibc.com
Tel: +91 (0) 124 502 6059

DOING BUSINESS IN INDIA HELPLINE
For support call +44 (0)20 7592 3040

WEBSITE
www.ukibc.com