BIF SUBMISSION/COMMENTS ON DRAFT PERSONAL DATA PROTECTION BILL 2018

BIF
Broadband India Forum

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The report on Data Protection by the Justice Sri Krishna Committee and the draft Data Protection Bill 2018, are historic first steps that could help secure the digital future of India's connected citizens. Broadband India Forum appreciates & welcomes the opportunity provided by Ministry of Electronics & IT (MeitY) to offer its comments to the draft Data Protection Bill.

A central theme of data protection reform worldwide, has been the two-fold ambition to afford individuals the right to 'regain control of their data', and to design solutions & policies that enable the economic and social potential of digital technologies[1]. And while there exist numerous justifications for considering privacy a fundamental right, the landmark 2017 judgment of the nine-judge bench in Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors.[2] renders the suitable implementation of appropriate data protection rules an absolute necessity.

Operating within similar objectives, the committee has masterfully articulated what it would take to bring the nation closer to protecting the privacy of its citizens in the digital age. While an admirable treatment of the complex exercise has been accomplished and the Justice Sri Krishna Committee deserve great kudos for this, there are a few aspects that are critical for the development of a thriving market for digital services that could do with increased clarity and a slightly more optimal treatment.

The major objective of protecting individual privacy has generally been addressed well in the report and the draft bill, and while much of it must be retained in its current shape & form, issues such as data localisation & cross border data flows are areas that could benefit from a review. ***BIF strongly subscribes to the view that data localisation should not be mandated, for an emerging or growing economy, on a carte blanche basis across all types and categories of data. Data localisation is an eminently desirable objective that may be pursued and supported for introduction at the optimum juncture in a nation's growth trajectory, after accounting for relevant policy considerations.. For example, these include policy reforms and economic incentives for attracting investments in the data centre industry. Until such time,*** **certain critical categories of information like defence or national security** ***data can be mandated for local storage***

In a growing nation like ours, to mandate this for all data would be to seriously disadvantage the very large community of startups and MSME's,for whom the higher costs involved would harm profitability and their very survival in a highly competitive and price-sensitive market like India. Large corporations would have the

[1] EP Press Service (2016) Data protection reform: Parliament approves new rules fit for the digital era. Strasbourg: European Parliament.

[2] Complete Judgment available at https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

wherewithal to make the investments and push ahead, passing on part or whole cost increase to the customer. Startups and MSMEs will not be able to do this and would therefore be compelled to fold their tents and exit the market – clearly, not a desirable outcome. We believe that an overly prescriptive governance framework, and a penalty structure that can charitably be described as dis-proportionate, warrant re-examination since such approaches have hardly ever given consistent good results. A heavily regulated data protection regime, such as the one currently under review, will significantly reduce the incentives to invest in innovative technologies such as AI & IoT, and may well keep Digital India from achieving its true potential. It has also been suggested with a reasonable degree of clarity that failure to address these issues may even be to the detriment of consumers.

BIF strongly believes that balancing these priorities is well within the realm of the possible, and that minor changes, motivated by the nuances of digital markets, will enable the creation of a set of business-friendly policies that maintain strong provisions to protect the fundamental and inalienable right to privacy. We argue this case based on the following core principles

- **Data Protection is best approached with the goal to balance two priorities** – securing individual privacy rights and promoting the growth of digital technologies
- **These priorities are compatible:** Data driven innovation can't be scaled without adequate privacy safeguards and gaining users' trust. The law needs to find the right balance between protecting the rights of the individual and enabling innovation. Strict regulations such as localization mandates neither ensure privacy nor support innovation and entrepreneurship.
- **Data localisation is certainly worthy of pursuit:** As already stated earlier, the localisation of Indian data, and the hosting of International data, within the territory of India, is a worthy goal to pursue. The spillover effects of investment in datacentres are significant when one considers the size of the Indian market alone, and orders of magnitude higher when accelerated by a thriving market that can cater to the requirements of foreign markets. This localisation however is an achievable goal if & only if it is economically viable to store data within the nation. Mandates to localise information do not improve security, as is often the justification for such policies, and according to several analyses, are directly linked to reductions in total factor productivity across industries, as well as a lower real GDP. Apart from the aspect of economics, one must consider that mandated setting-up of data centres would divert power from important areas of consumption which are already suffering from short supply and thus harm the overall interest of the general public and the economy.
- **Cross-border data flows are part of the modern Internet's DNA:** The decentralized nature of the Internet is fundamental to its success, and its proven ability to catalyse innovation. Mandates that prescribe manners and methods to structure data flows can potentially ignore the decentralized economics that made the Internet successful. New & novel technologies such as AI would conceivably require access to vast amounts of data on a continuous basis to learn and become smarter/intelligent. India's IT sector, start-up & developers community will benefit greatly from affordable access to data – regardless of what country the data resides in. A regulatory regime that supports cross border data flows, and adopts an economically pragmatic view of the costs of data storage will accelerate innovation, to the ultimate benefit of consumers. At the same time, security should be of paramount import to any policy on data protection.
- **Security should not be compromised for innovation:** Data innovation and security should go hand in hand and security should never be compromised. We are of the view that security of data is not a function of where it is stored, but rather how data flows meet international standards. Ultimately security of data is truly more a function of the processes put in place, the access controls granted, data classification implemented, etc. as opposed to where the data is located. Data localization is often misidentified as a driver of security, whereas cyber-attacks are global in nature and target vulnerabilities and unmanaged IT environments regardless of where the data is stored.

Keeping the above principles in mind, we offer normative recommendations on the following issues given below which we urge Ministry of Electronics & IT (MeitY) to kindly consider prior to finalisation of the Draft Bill.

1. Data localisation mandates & cross-border data flows
2. Overly prescriptive governance, disproportionate penalties & wide powers of the DPA
3. Bill's harsh penalties & criminal offences will prevent effective enforcement
4. Definitions in need of review
    a. Sensitive Data
    b. Biometric Data
5. Notification requirements and purpose limitation
6. Privacy by Design
7. Data Breach notifications
8. Grounds of processing of data
9. Processing children's data
10. Consent for Minors
11. Data Storage Limitation
12. Unclear Transparency and Accountability Measures
13. Anonymisation
14. Processing for Research, Archiving or Statistical Purposes
15. Prohibition on Re-Identification
16. Applicability
17. Significant Data Fiduciaries
18. Data Protection Obligations on Significant Data Fiduciaries
19. Extra-territoriality

Our detailed response to each of the above points are given below :

1. DATA LOCALISATION MANDATES & CROSS BORDER DATA FLOWS

BIF supports data localization as below:

We sincerely believe that data localisation should be encouraged and incentivised such that it becomes the automatic optimal choice from the overall point of view that includes operational efficiency, enhancement of competition, reduction of end-customer costs, encouragement of innovation , startups & MSMEsetc. Certain categories of data like related to defence, national security and such should continue to be mandated but not a compulsory localisation of all data types. We believe to mandate localisation of data would drive up costs for startups and MSMEs and reduce affordability for end-users.

The Bill specifies that every data fiduciary shall ensure the storage, on a server or data centre *located in India*, of *at least one serving copy* of personal data (Clause 40). Under the Bill, the Central Government shall notify categories of personal data as 'critical personal data' that shall *only* be processed in a server or data centre located in India (Clause 41). Such data is not permitted to be transferred outside of India at

all. The Report of the Expert Committee suggests that such 'critical data' means 'data relating to critical state interests', such as Aadhaar number, genetic data, biometric data, health data, etc. (pg. 93 of the Report). The only exception for transfer of critical personal data is for sensitive personal data notified by the Central Government which may be transferred outside the territory of India— (a) where such transfer is strictly necessary for prompt action, to a particular person or entity engaged in the provision of health services or emergency services; and (b) where the Central Government is satisfied that such transfer or class of transfers is necessary for any class of data fiduciaries or data principals and does not hamper the effective enforcement of this Act, to a particular country, a prescribed sector within a country or to a particular international organisation that has been prescribed as permissible by the Central Government.

These requirements are out of step with privacy legislation elsewhere in the world and increases compliance costs, while reducing agility for innovation and offers no corresponding benefit to data principals. For example, while the GDPR has specific and detailed requirements for transferring personal data outside of the EU, it does not have any requirements for a copy of personal data to be stored in the EU. In fact, the preamble of the GDPR states: "Flows of personal data to and from countries outside the union and international organisations are necessary for the expansion of international trade and international cooperation".

The Bill also requires that every data fiduciary maintain at least one serving copy of personal data on a server/datacenter in India, with some discretionary exemptions based on necessity and strategic interests of the State. Sensitive personal data and critical personal data are governed by even more restrictive positions.

Even when cross border flows are allowed, the Bill mandates DPA approved standard contractual clauses, intra-group schemes and adequacy determinations for such transfers in addition to data principal' consent. The imposition of such requirements is fraught with concerns, especially around their subjective and unilateral nature. Further, such a framework is in sharp contrast to India's commitment to improving the ease of doing business in the country which predicates easy and unfettered access to flow of data for business purposes. Across sectors, there is a marked move to reduce regulatory interface, and this rationale should be extended to open, transparent and contractually guided cross border data flows, especially given the reliance placed upon cross-jurisdictional engagements in most sectors. For example, in the EU, companies are known to have taken anywhere from 11 months to over 3 years to get approvals for intra-group schemes.[3] The Indian IT industry already suffers due to such interventions by the EU, and this is not a model India should try and replicate. NASSCOM, as the representative of the IT/ITeS industry in India has already highlighted the challenges faced by Indian firms in complying with the adequacy requirements of EU. According to a NASSCOM survey, for just 15 companies in the Indian IT industry, the estimated loss of business due to the EUs prescriptive adequacy data protection regime was $2 billion+ dollars.[4] This impact will be exponentially greater for the entirety of India's IT sector. These restrictions have the potential to significantly harm India's standing in the global stage from the standpoint of economic growth, market competitiveness, consumer access, and international obligations.

The Bill also sets out a very limited basis on which personal data (other than sensitive personal) can be transferred outside of India. On one interpretation the only permissible bases are: (a) transfers subject to standard contractual clauses or intra-group schemes approved by the DPA, (b) transfers to 'whitelisted' countries, or (c) transfers that the DPA approves on the basis of necessity. The intended purpose of grounds (d) and (e) set out in Clause 41 is unclear and the Bill should clarify whether consent will always be required for grounds (a) and (b). Such bases are much narrower than other jurisdictions and as

[3] Binding Corporate Rules, Allen and Overy. Available at: http://www.allenovery.com/SiteCollectionDocuments/BCRs.pdf

[4] NASSCOM Update on EU Data Protection Regime. Available at: https://www.nasscom.in/sites/default/files/policy_update/EU%20data%20Protection%20Regulation.pdf

discussed above will significantly restrict cross-border flows to data to the detriment of both businesses and individuals. It is unclear why personal data can only be offshored in these narrow circumstances. The Bill should be amended to include additional grounds on which personal data can be offshored, so long as the data fiduciary remains responsible for its protection and no additional consent should be necessary. For example, in the Philippines there is no restriction on the transfer of personal data outside of the Philippines but the data controller remains responsible for the protection of the personal data. Similarly, in Australia organizations are responsible for taking reasonable steps to ensure that the overseas recipient of personal data does not breach the Australian Privacy Principles and the transferring organization remains accountable for the overseas recipient's acts. The GDPR also provides the following grounds for transferring personal data offshore: (a) binding corporate rules, (b) legally binding instruments between public authorities, (c) approved certification mechanism together with binding and enforceable commitments to apply appropriate safeguards.

ECONOMIC IMPACT OF DATA LOCALISATION

The current provisions of the Bill will negatively impact India's market competitiveness by harming the key pillars of its GDP: start-ups & micro, small and medium enterprises (MSMEs). India currently boasts of the 3rd largest base of start-ups in the world while MSMEs contribute approximately 37.5% of India's GDP. Cloud computing services are affordable for consumers and small businesses/start-ups because they rely on massive economies of scale with globally distributed datacentres. Requiring data centres to be located domestically dramatically undermines the cost-effectiveness of cloud-based computing services and reduces the choices available to India's homegrown technology sector. MSMEs should have an option on whether to use domestic cloud service providers or foreign providers depending on the quality of services and competitiveness of the cost besides reliability and data security. Otherwise, Indian MSMEs will suffer from disadvantage of losing access to globally available cloud resources while MSMEs in other countries will enjoy the benefits of ample cloud infrastructures as well as significant transborder investments. Data localisation will also place significant pressure on the government from a technical, financial and regulatory environment standpoint to create local infrastructure for smaller players. It is of paramount importance that we need access to international markets to build our solutions and for the burgeoning ITES Sector to thrive.

According to a 2014 European Centre for International Political Economy (ECIPE) study, an economy-wide data localisation measure would have caused a GDP loss of -0.8% for India. It would also lead to a loss of approximately 11% of the monthly salary of an average worker. In addition, the domestic and foreign direct investment (FDI) that drive Indian exports and long-term growth, would drop by -1.9%. Given India's rapid development, these hard-hitting statistics are bound to only have increased over the past few years. All of this data showcases the integral value that cross border data flows have created for the Indian economy. Any hindrances to such cross-border data flows would adversely impact innovation, economic competitiveness, foreign investment and availability of affordable technology to users across the country.

Another 2016 study by the Centre for International Governance Innovation reveals that under a relatively liberal data localisation mandate than the one under discussion currently, India may stand to take a .25 percentage point hit to its real GDP. According to the report, *"communication services sectors show large productivity losses due to their high dependency on data inputs covered by data regulations. Data-intensive business and financial services also show relatively high losses in productivity. As concerns economic output, the production of data- intensive manufacturing and services sectors shrinks in all countries due to regulations on the free flow of data. Losses are notably taking place in the services sectors. The greatest declines in industry output are found for communications and business services, but also for financial services. At the same time, less data- intensive sectors are less affected by data regulations. The general patterns in the results indicate a shift in production from the services and manufacturing to the primary sector as a result of restrictions on the flow of data. Accordingly, tight regulations on the free flow of data tend to cause an*

economy's production structure to shift (back) toward less innovative and relatively volatile sectors such as agriculture, raw materials and natural resources"[5].

According to a 2016 Mckinsey report, data flows acting together have raised world GDP by 10.1 percent over what would have resulted in a world without any cross-border flows. The value amounted to some $7.8 trillion in 2014 alone, and data flows account for $2.8 trillion of this impact. This impact is greater than the global flow of goods in the equivalent period. Particularly for India, cross border data flows have been critical for the establishment and growth of its outsourcing (ITES/BPO) sector. India's IT-BPM industry, which has been founded on the global free flow of data, accounts for 55% of the world's outsourcing market and is worth US$ 173-178 billion. The IT-BPM industry has a share of 45% in India's total service exports and contributes ~7.9% to India's GDP. This industry also employs a workforce of approximately 10 million workers in India. Actions to restrict cross border data flows will seem duplicitous on India's part due to the benefits it has reaped from such flows in the past. Such actions could attract reciprocity from other nations who trust their data with us and thus could therefore directly lead to a reduction in India's standing on the world stage thereby harming growth of the economy, reducing available jobs and hamper foreign investment.

Studies have indicated that prohibiting cross border data flows in the form of data residency requirements can impact local and regional economic growth and competitiveness in the global market, with the greatest impact being borne by SMEs.[6] A 2015 study by an information security company, showed that the cost of IT services can substantially increase due to data localization, depending on the availability of alternative services.[7] SMEs, including start-ups which are some of the most innovative players in the Indian market, are likely to be most impacted by these increased compliance costs which could stifle innovation and entrepreneurship in India.

Data localization also limits the ability of Indian companies from fully realizing the benefits of hyperscale cloud services such as improved resiliency, availability and agility, while at the same time benefiting from economies of scale. Leading hyperscale cloud service providers, like AWS, offer customers the opportunity to build adaptive and highly resilient security for their workloads. Restricting operations to specific in-country requirements would inhibit service innovation and hinder the ability to compensate for threats, such as ones that target availability. Another detrimental by-product of in-country geographic constraints is that threat actors can gain targeting accuracy knowing the data must reside within specific areas. Hyperscale cloud service providers have available offerings and supporting architectures to offer both defence in depth and defence in breadth capabilities. This is due to security mechanisms being intrinsic to the design and operation of hyperscale cloud service provider offerings.

The following India specific illustrations, each of which have cross border flow data at their core, can serve as potential examples of possible losses that can occur to the Indian economy if the draft bill were to be implemented in its current state:

- India's net exports from its IT sector accounted for over U.S. $117 billion in fiscal year 2016-2017[8]. Meanwhile, India's big data analytics sector in India is expected to witness an eight-fold growth to

---

[5] Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization, May 2016, Centre for International Governance Innovation, available at https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf

[6] https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows;

[7] Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" Information Technology and Innovation Foundation (May 2017) http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.243762501.1722557619.1508762047-1611916082.1508762047.

[8] India's IT-BPM industry crossed $150 billion in 2016-17, Livemint. Available at: https://www.livemint.com/Technology/yU4vKtK5rS2yQWCzJpRPYM/Indias-ITBPM-industry-crossed-150-billion-in-201617.html

reach $16 billion by 2025.[9] This inflow, largely based on free-flowing data, would be severely restricted by requiring data localisation from all players wishing to offer services in and from India.

- According to a BIF-ICRIER Report[10] it is estimated that mobile apps, which are overwhelmingly hosted outside India, contributed a minimum of USD 20.4 billion in 2015-16 to India's GDP, and this contribution is expected to grow to USD 270.9 billion by 2020. This would be nearly 8% of India's GDP. The study also finds that while a 10% increase in total free flowing Internet traffic and mobile Internet traffic globally increases global GDP by 1.3% and 0.7% respectively, *for India the impact is much higher.* In India, a 10% increase in free-flowing total Internet traffic, delivers on average a 3.3% increase in India's GDP. Enforcing data localisation requirements on app developers, which are largely individuals or startups, would massively reduce this substantial economic impact due to increased compliance costs. This would also have a chilling effect on domestic bootstrapped innovation by imposing a high barrier of entry for new local entrants in a wide range of sectors in the Indian market.

- According to an Accenture report[11], artificial intelligence, a key focus for the Indian government, is expected to raise India's *net annual growth* rate by 1.3 percentage points by 2035. This amounts to an addition of US$957 billion, or 15% of current gross value added, to India's economy by 2035 when compared with a scenario without AI. Restricting the cross-border flow of data would not only prevent the inflow of data crucial for training datasets but also block access to the Earth scale storage and processing power required to drive AI technologies in a fruitful manner. This would conflict with the Govt's vision to make India a superpower in artificial intelligence as articulated in the Niti Aayog White Paper on AI, by being an 'AI Garage for Emerging Economies'[12]

- According to a McKinsey report, 80% of tech-based start-ups worldwide are "born global" utilising foreign customers, financing, suppliers from day one. In a global start-up survey, 86% of respondents pointed to at least one cross-border activity. Almost two-thirds have customers or users in other countries, and almost half reported sourcing manpower resources from other countries. Enforcing restrictions on cross border flows will hinder the ability of India start-ups to compete with their global counterparts due to unique increased costs and compliance burdens they will have to undertake unlike their global counterparts. These restrictions will also reduce the inflow of foreign investment such start-ups bring to India by reducing their attractiveness to investors.

- It is estimated that there are around 51 million Micro, Small and Medium Enterprises (MSMEs) in India which contribute 37.5% to India's GDP. 68% of the 51 million MSMEs operate offline in India today. According to a KPMG report, the digitization of MSMEs could help increase their contribution to India's GDP by 10 percentage points, taking it up to 46-48% by 2020. Affordable cloud-based online tools are already helping Indian MSMEs drive their exports and cross border data flows are fundamental to this development. It is estimated that cutting off access to global cloud computing services— through localization— would force local companies in Brazil and the EU to pay 10.5 to 62.5 percent more for some cloud computing services. According to the World Bank and OECD, about 43 percent of Indian export oriented MSMEs depend on online tools for 75 percent of their global sales.

---

[9] Big data analytics to become $16 billion industry by 2025, Economic Times. Available at: https://economictimes.indiatimes.com/tech/ites/big-data-analytics-to-become-16-billion-industry-by-2025/articleshow/59410695.cms

[10] Estimating the Value of Internet New Generation Based Applications in India, ICRIER. Available at: http://icrier.org/pdf/Estimating_eValue_of_Internet%20Based%20Applications.pdf

[11] Rewire For Growth: Accelerating India's Economic Growth With Artificial Intelligence, Accenture. Available at: https://www.accenture.com/t20171220T030630Z__w__/in-en/_acnmedia/PDF-68/Accenture-ReWire-For-Growth-POV-19-12-Final.pdf#zoom=50

[12] National Strategy for Artificial Intelligence, Niti Aayog. Available at: http://niti.gov.in/content/national-strategy-ai-discussion-paper

Mandating data localisation provisions will drive up the costs incurred by MSMEs in utilising digital tools, reduce their odds at effectively competing with their global counterparts and lock out free access to global markets.

- According to a Fifth Era report, 81 percent of investors who responded to a survey for the report said they are uncomfortable investing in internet business in India if the enterprises are obligated to store user data on servers located in India and/or build their own data centres locally.
- The business decision to locate a cloud datacentre in a country is driven by various factors including revenue/market potential, internet connectivity, legal frameworks, etc. These factors especially include privacy laws, cross border data flows, lawful access to data, reliable and renewable energy, climate, law and order situation, political stability, etc. Several of these parameters need to be significantly improved for India to become a global hub for cloud services. To move large data centres to India would require huge amount of power and cooling, which would require a humungous amount of energy (power) & space mobilization and would ultimately culminate in costs that are several orders of magnitude higher than economically optimal choices.

It is true that India offers inherent cost advantages for certain business activities, which is made possible by the free play of market forces. When the government makes heavy-handed interventions in the market, it interferes with the same market forces that enable economies of scale and cost advantages. As the Indian digital sector grows, the market will incentivise the setting up of data centres in India when market conditions are optimal. At the moment, the cost of setting up data centres anywhere in the world is very high -- and it will be higher in India because of the added costs of infrastructure (e.g., guaranteed uninterrupted power supply) that India is unable to provide. Therefore, market conditions are not optimal for data localisation. Forcing companies to incur these huge additional costs will severely affect the competitiveness of Indian companies and will undermine India's attractiveness as a global investment destination and business centre.

Forcing data localisation will not automatically create the technical, financial and regulatory environment conditions needed for local data centres to emerge in India. Organic incentives are a more sustainable way to ensure that all the relevant levers shift in consonance for lasting growth rather than imposing forced demand onto a delicately balanced ecosystem. This is likely to lead to increased costs and a decrease in the reliability of service.

If the data localisation requirement proposed in the Bill is retained it may disincentivise international companies from offering services within India, because it may be too costly or otherwise impractical to do so. Individuals in India will have fewer choices as a result.

Data localisation requirements imposed by India would be likely to receive retaliatory localisation measures by other countries. This would negatively affect Indian national interest.

DATA LOCALISATION & SECURITY

One of the key drivers for data localization is the perception that lawful access to data would be facilitated, especially given the Mutual Assistance Legal Treaty (MLAT) process is broken. This is based on an incorrect understanding of applicable legal and regulatory framework. Merely hosting data in a

particular jurisdiction does not increase the lawful access of such jurisdiction to such data, especially due to conflict of laws from jurisdictions in which parent organisation that may have custody, ownership and control over such data are registered, location of encryption keys, etc. Further, it is well documented that even currently, access to data for lawful/legitimate purposes is enabled and made possible without a requirement of physical location of data. It is not clear what specific problems of lawful access are addressed by provisions that restrict cross border flow of data. **In the cloud era, countries that honor baseline principles of privacy, human rights, and due process should be able to efficiently access data (irrespective of where it is stored) that pertains to serious crimes that happen within their borders and users who are within their jurisdiction**. Approaching this issue by mandating data localisation, which does not guarantee desired outcomes (due to legal and jurisdictional complexities) will only lead to negative economic impacts and little in the way of ensuring security. Further it would also be prudent to allude to the recent Supreme Court Ruling on Aadhar Act where in by striking down section 33(2), the Honourable Supreme Court has clearly brought privacy of citizens data to a very high bar. Further the honourable Supreme Court has laid emphasis to a clear process with judicial oversight to provide access to data even in the case of National Security which lays the basis for evaluating similar processes for access under the Data Bill and not Data Localisation.

We believe that data that is critical to the nation's interest should remain within the nation's control. However, such data is already covered under various data localisation requirements that are sectorally or specifically applicable. For instance, (i) Defence Ministry regulations mandate that certain security-related data remain in India; and (ii) the Public Records Act mandates that official government records cannot be taken outside India (the Delhi High Court has extended this requirement to data that is stored online). There are also existing provisions for data localisation for sensitive customer information. For instance, (i) telecom service providers governed by the Universal Licence are required to store user data and subscriber data in India only; (ii) the Insurance Regulatory and Development Authority requires the primary servers of insurers to be located in India; and (iii) the Reserve Bank of India requires core banking information to be stored in India.

The Government of India has a legitimate need to take measures to protect national security and enforce law and order. However, data localisation and restriction of cross border data flows are not the best way to address the needs of national security and law enforcement agencies (LEAs). This is simply because data localisation does not guarantee access to data. The best way to secure data access for LEAs is for the Government of India to enter into data sharing and cyber cooperation agreements with friendly governments. For instance, the 2016 US-UK Cybersecurity Cooperation Agreement gives LEAs and national security agencies from those countries guaranteed cooperation and access to data within short timeframes. Moreover, in 2018 the US enacted the CLOUD Act, which enables India and the US to easily enter into an agreement to allow data access to both governments irrespective of where the data is stored.

Data protection does not generally depend on where the information is stored, but rather what measures are used to secure the data. A secure system in India is no more or less secure than a similarly architected system in the EU. Physical location generally has no relevance because data centres are almost always connected to broadly accessible networks, and thus real security depends on technical, operational, and managerial practices implemented by the data fiduciary and the data processor. For example, data fiduciaries can implement strong encryption practices that make the personal data unreadable in the case of unauthorized access or malicious activity.

DATA LOCALISATION & PRIVACY

In light of the existing data localisation provisions for critical data and sensitive customer information, it is felt that there is perhaps no need for any further laws in this area. Moreover, there is absolutely no need for a blanket data localisation law because the bulk of the data that it will cover is neither critical data nor sensitive customer information. Because the data localisation provisions in the Draft Personal Data Protection Bill ("Draft PDP Bill") are extremely widely drafted, it will severely affect harmless data processing by ordinary businesses, which are the backbone of India's digital economy.

The Draft PDP Bill contains strong safeguards for data privacy and data security, which apply to all data that is collected in India, including by foreign companies operating in India. The law is expected to sufficiently protect the privacy interests of the consumers. Data localisation has no connection to privacy or security. Removing the data localisation sections from the Draft PDP Bill will make absolutely no difference to user's data privacy and data security, which are already well protected.

DATA LOCALISATION & CONSUMER INTEREST

Cross-border data flows have enabled universal access to information by empowering individuals across the world. The global nature of the Internet has democratized information which is available to anyone, anywhere in an infinite variety of forms. The economies of scale achieved through globally located cloud infrastructure have contributed to the affordability of services on the Internet, where several prominent services are available for free. Companies can provide these services to users even in markets that may not be financially sustainable as they don't have to incur additional cost of setting-up and running local data centers.

Globally, over 900 million users have international connections on social media, showcasing the interconnected nature of modern social interactions. All these users will be negatively affected by restrictions on cross border flow of data due to the siloed nature of localised technical infrastructure. The current form of the Bill also leaves a large scope for the violation of privacy rights of end users given exemptions for data processing by government and the proportional increase in surveillance capabilities when data is located in the country. Therefore, restrictions on cross border flow of data will harm consumer experience on the open internet, increase costs and leave them more susceptible to issues of security, reliability and unlawful access. Other relevant factors from an end user point of view include:

- Storing data across jurisdictions increases security and reliability and is helpful in business continuity during natural disasters where all local infrastructure may be damaged. Factors behind this include the fact that technical security expertise is expensive and rare, systems are generally harder to update with the latest security software and storing data in one location could create a more attractive target for foreign surveillance as well.
- Data localization also prevents citizens of the country from accessing innovative offerings.[13] For instance, data localisation of medical data in Australia, Canada, China, and Russia hampers access to innovative technology to patients.[14] Data localization also hinders international medical

[13] Nigel Cory, Cross-Border Data Flows: Where are the Barriers, and What Do They Cost?, Information Technology & Innovation Foundation, 8 (May, 2017) available at http://www2.itif.org/2017-cross-border-data-flows.pdf (Last accessed on 5th August, 2018).

[14] *ibid*

research as it discourages exchange of medical data[15] including outsourcing of data related to magnetic resonance imaging.[16]

- The legal due process for lawful interception and surveillance need significant reform in India to protect civil liberties of its citizens. For example, the government committee that is mandated to review requests under Section 69 of the IT Act meets at least once in two months. However, an application under the Right to Information Act to the Ministry of Home Affairs[17] has revealed that on an average 7500 to 9000 orders for interception are issued every month by the Central Government alone. Therefore, if the review Committee meets once every two months as it is statutorily mandated to do, then it would have to consider and dispose of between 15000 to 18000 orders of interception at every meeting. This showcases the vast regulatory gap that requires ground up reform in the form of independent, transparent and principle based judicial oversight of lawful interception. The belief that data localisation improves lawful access to information by the state authorities is incorrect
- We witness processing of high volumes of personal data daily in several forms like "likes" and preferences on social media platforms, search engine prompts, and likewise. Unless anonymized, as per the requirements under the proposed structure this will have to be mirrored and a serving copy of the same will have to be retained in India. This ask, has spilled concerns all over, pertaining to the costs which are expected to be incurred, and the efficiency of such move. For the purposes of 'critical personal data' which is yet to be defined, Section 40(2) affords the Central Government to specify the categories; and has imposed strict data localization norms on such category. While it is to be noted that not all sensitive personal data qualifies as 'critical personal data', there is a lot of ambiguity as to the data localization norms in respect of sensitive personal data.

DATA LOCALIZATION AND INTERNATIONAL LAW

Data localisation and the resultant trade barriers can undermine India's obligations under international treaties such as GATS at the WTO[18] and other upcoming regional trade agreements such as the RCEP. The provisions as currently drafted may not meet the various threshold criteria such as of objectivity and reasonableness as laid down in GATS. In fact, India has for long been demanding that EU relaxes data flow strictures imposed on India under the upcoming India-EU Free Trade Agreement[19] It is important to note that even the EU does not mandate across the board data localization and in fact has a framework for protecting the free flow of data in its single market.[20] Imposition of such discriminatory requirements can also potentially provoke retaliatory measures from other governments in the form of tariffs or restrictions that can harm the Indian IT industry, and other sectors, given ongoing trade tensions. It is also important to note that India's trade partners in developed markets in Asia Pacific, such as Japan and Singapore, are endorsing free trade principles based on international frameworks of cooperation. They

[15] Daniel Castro and Alan Mcquinn, Cross-Border Data Flows Enable Growth in All Industries, Information Technology and Innovation Foundation, 11 (February, 2015) available at http://www2.itif.org/2015-cross-border-data-flows.pdf

[16] Keynote Speech by the Deputy Secretary-General of UNCTAD, Harnessing the Digital Economy for Economic Growth and Development, UNCTAD E-Commerce Week, 3 (18th April, 2016) available at http://unctad.org/meetings/en/Presentation/dtl_ict4d2016eWeekp01_Reiter_en.pdf

[17] ORF Special Report: Hitting Refresh Making India-US Data Sharing Work. Available at: http://cf.orfonline.org/wp-content/uploads/2017/08/ORF_SpecialReport_39_DataSharing.pdf

[18] Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments, Daniel Crosby. Available at: http://e15initiative.org/wp-content/uploads/2015/09/E15-Policy-Brief-Crosby-Final.pdf

[19] India asks EU to address concerns on data security status, Livemint. Available at: https://www.livemint.com/Politics/hMwanvZOn84vuGU4jr4kxH/India-asks-EU-to-address-concerns-on-data-security-status.html

[20] Regulation Of The European Parliament and Of The Council on A Framework For the Free Flow of Non - Personal Data in the European Union. 2017/0228 (COD). Available at: http://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-495-F1-EN-MAIN-PART-1.PDF

understand that the free data flow is a crucial principle in order to allow access to multiple markets. These countries are also endorsing Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Regional Comprehensive Economic Partnership (RCEP) as well as APEC Cross Border Privacy Rules (CBPR) to enable cross border data flows while protecting privacy. If India prematurely forecloses its ability to participate in such agreements, it will lose out on the vast free trade generated by them, leading to a lost opportunity.

RECOMMENDATIONS:

a. *The Bill should abstain from regulating the free cross border flow of data in any form to prevent the negative impact detailed on the country, its growth and the consumers. Besides it is likely to have negative effect on India's economy, international standing and consumers alike.*
b. *If the government does plan on regulating data flows, it should restrict data flows or explore localization norms very conservatively and only where necessary to achieve very specific policy goals in sensitive sectors that are specified. Such restrictions should also be designed and applied in a non-discriminatory, least trade restrictive and transparent manner. With regard to DPA approved standard contractual clauses, intra-group schemes and adequacy determinations, a universally acceptable and equitable alternative is data transfers based on comparability. Under existing laws in India (IT Act) (specifically, the Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011) data may be transferred to another entity locally or overseas so long as the receiving entity has in place security practices that would be considered compliant under the relevant Indian law. These are the same requirements that every domestic entity is required to comply with, hence the treatment accorded to local and international entities is fair and equitable without being unnecessarily bureaucratic. The government should also look at alternative instruments for unrestricted trans-border data transfer under internationally agreed frameworks, trade agreements or economic cooperation frameworks such as CPTPP, RCEP and APEC CBPR.*
c. *To address lawful access to data issues, the government should engage through bilateral and multilateral instruments and make data sharing work in the cloud era without resorting to data localization measures. For example, the CLOUD Act recently enacted by the U.S. enables bilateral agreements for qualifying countries which would allow non-US qualified governments to seek data in a much more efficient way. India should aim for such an agreement to resolve issues while limiting the negative economic impact of localisation and this would, among other things, require enhancing privacy safeguards around lawful access to data.*
d. *The Bill should contain the provisions that enable judicial interventions, review and oversight for surveillance and lawful access to data to oversee processing carried out by the government, with or without consent. The legal regime should enhance privacy safeguards based on the sensitivity of the data being accessed/intercepted (e.g. content versus non-content data) by the government. It would also help in enhancement of privacy standards to oversee that collection of data by the State is reasonable, proportionate, transparent and minimally intrusive.*
e. *The Bill should consider the consent of the data principal as adequate authorisation for cross border transfer of data. Therefore, it is recommended that Section 41(3)(d) be amended to delete the words 'in addition to clause (a) or (b) being satisfied.'*
f. *The Bill should incorporate broader grounds on which personal data can be transferred offshore to be more consistent with international practices, including allowing data to be transferred offshore as long as the transferor has taken reasonable steps to ensure the recipient will apply appropriate safeguards and the transferor remains accountable for the protection of the data. No additional consent should necessary for the transfer of personal data offshore so long as the data fiduciary has complied with its consent and notification obligations. Moreover, the DPA should expedite the approval of the "standard contractual clauses" [the language of these clauses should be determined in partnership with the industry drawing in relevant aspects from the Contracts Act and could be modelled on the lines of what is included in the EU GDPR] and countries that it determines have an appropriate standard of protection to provide additional clarity to all parties involved.*

With these concerns in mind, we urge the Government to refrain from adopting any form of data localisation or restriction on cross-border data flows. Where localisation is necessary to achieve specific security or strategic

objectives (for e.g. in relation to defence), the government must include a specific list of statutory criteria or conditions within the Draft Bill, which will guide discretion in notifying types of data which may need to be stored within India.

2. OVERLY PRESCRIPTIVE GOVERNANCE, DISPROPORTIONATE PENALTIES & WIDE POWERS OF THE DPA

The enforcement envisaged in the Draft Bill is problematic due to an overpowered DPA, a highly prescriptive governance framework and steep criminal penalties. The DPA has wide prescriptive, discretionary and onerous powers under the Bill. These include the powers of a civil court such as issuing directions, seeking information, initiating inquiry, search and seizure, and adjudication. Technology developments are dynamic and attempts to monitor for compliance will likely place significant, if not overwhelming, burdens on any government agency entrusted such a charge. Instead of nurturing the technology ecosystem as intended, this load will ultimately harm consumers, businesses and the government equally. A restrictive data protection regime is also not aligned with Indian culture, values and attitudes[21].

Penalties under the Bill range up to INR 150,000,000 or 4% of the worldwide turnover and allow for imprisonment sentences of up to 5 years. There are unnecessarily harsh, disproportionate and will stifle the Indian economy. The Supreme Court in *Excel Crop v. CCI*[22] has laid down detailed norms on the doctrine of proportionality as applicable to corporates. It was observed: "...The doctrine of proportionality is aimed at bringing out a proportional result..." It is a result-oriented test that ensures proportionality achieves a balancing act between two competing interests: harm caused to society and the right of the infringer in not suffering punishment which may be disproportionate to their act. Applying the penalties in the Bill on global turnover and including would defeat the principle of proportionality and create a chilling effect on any start-up, firm or corporation that would want to operate or offer its services in India. Some of the reasons for this are:

Data protection impact assessments (DPIA), appointment of a data protection officer (DPO) and data audits by an independent auditor, all of which need to be reported to the DPA, are some of the heavy-handed accountability measures outlined in the Draft Bill. Privacy, as illustrated below, is a subjective construct. Different sectors of the industry utilise different types of data and depending on their sensitivity, industry privacy practices are best developed specifically for such sectors, such as banking, insurance, health, travel, education etc. It is, therefore, unreasonable to expect its compatibility with the excessively objective criteria outlined in the Bill for the following reasons:

- These requirements are extremely prescriptive, and therefore likely anti-innovation. A privacy impact assessment is primarily a tool to help an entity identify effective modes of compliance with data protection and privacy obligations. Data fiduciaries should be encouraged to conduct such internal assessments and have internal points of contact as a good practice of ensuring awareness, both within the company and with respect to users, at the organizational level. However, conducting such assessments in order to gain permission to use new technologies or provide services based on processing, and appointing a DPO located in India, creates a heavy handed regulatory regime, as opposed to a liberal, pro-innovation one.

---

[21] Privacy and the Indian culture, Livemint. Available at: https://www.livemint.com/Opinion/rM3vgXErD5oWiv12IEaKcK/Privacy-and-the-Indian-culture.html

[22] *Excel Crop v. CCI* 2017(6) SCALE 241

- Only significant data fiduciaries maybe mandated by the DPA to comply with more onerous transparency and accountable measures including DPIA, data audits and appointment of a DPO. Certain companies will be placed with higher compliance burdens as opposed to smaller contemporaries in such circumstances. Mandatory DPIA and annual data audits result in excessive compliance burden in the form of loss of time and money. The costs involved in onerous compliance will affect also start-ups disproportionately, by discouraging start-up growth and innovation within India as compared with other countries. Further, DPIA and data audits by registered data auditors will lead to avoidable regulatory intrusion in the personal data management practices of a data fiduciary. A newly formed DPA may not have the regulatory capacity, technical capability and resources to effectively perform such functions without creating a logjam of compliance related delays that would negatively affect both significant and other fiduciaries equally.
- The data trust scores by data auditors may suffer from subjectivity in the absence of benchmarks for consideration by the data auditors. Data trust scores based on codes of practice by the DPA may not reflect the comprehensive set of measures to provide additional safeguards due to the dynamic nature of data management practices. Additionally, data is controlled/ processed by millions of entities across the world. Establishing a systematic process of regulation mandated allocation of trust scores is both unfeasible and impractical. It also runs the risk of the user receiving incomplete or inaccurate information due to the sheer fragmentation with respect to availability and access to user information. Instead, the existence of a privacy-by-design approach should be assessed in order to arrive at a more accurate method of determining compliance with the law, with references to data trust scores being removed from the Bill
- Registration of significant data fiduciaries is an unnecessary provision that won't aid effective enforcement but will add additional delays to the government approvals required for organisations. In the UK for instance, there were about 4.9 million SMEs but only 370 thousand data controller registrations in 2014 questioning the practicality of such measures.

THE STRUCTURE AND POWERS OF THE DPA ARE UNNECESSARILY BUREAUCRATIC

The Data Protection Authority ("DPA") has been granted very broad discretion under the Bill both in terms of its powers but also in the implementation and application of the provisions of the Bill, with insufficient transparency or objective criteria contained in the Bill to act as a check and balance against this broad power. As a result, there is considerable uncertainty in how certain obligations will apply, to whom they will apply and how data fiduciaries and data processors are expected to comply with them. Specifically, the DPA has been granted the power for the following: (a) to identify other 'reasonable purposes' for which personal data can be collected and processed; (b) to designate entities as a 'guardian data fiduciary' or a 'significant data fiduciary' and thereby require them to comply with additional obligations under the Bill; (c) to specify additional categories of sensitive personal data which will then significantly restrict how such data can be collected or processed; (d) to mandate a time frame for responding to data principal rights requests; (e) to notify any additional information to be included in the 'notice' to customers, in addition to the statutorily mandated information; (f) to specify the criteria for assigning a 'data trust score'; (g) to determine when data breaches must be reported to the data principal; (h) to specify when data protection impact assessments are mandated; (i) to issue codes of practice on a very broad range of issues; (j) to approve intra-group schemes for transfer of personal data; (k) to adjudicate disputes; (l) to be subject to civil investigation including search and seizure, and for the determination of penalties and fines.

The DPA has also been vested with the power to issue directions from time to time to data fiduciaries or data processors generally, or to any data fiduciary or data processor in particular, and such data fiduciaries or data processors, as the case may be, shall be bound to comply with such directions (Clause 62).

The DPA is modelled like a more powerful and prescriptive version of the enforcement authorities under the GDPR. Establishing the DPA in its current form, as envisaged in the Draft Bill will lead to the establishment of

the erstwhile 'license raj' in the technology sphere in India. As an illustration of the harsh economic impact that can arise from such an outlook, before the EU GDPR was finalized, a Deloitte study[23] estimated its economic impact on the European economy. It suggested a reduction of the EU's GDP by € 173 billion (1.34% of GDP in EU-27) leading to a loss of 2.8 million jobs within a year of the GDPR entering into force. All of this impact was the combined effect from only four sectors: web analytics, direct marketing, online behavioural advertising and credit information. The increased size, scale and diversity of the Indian market will only magnify such numbers in India. Other relevant aspects of Bill in this regard include:

- The DPA is vested with broad, overarching powers to discharge quasi-executive, quasi-legislative and quasi-judicial functions. While there is a large mandate provided to the DPA, its limited institutional capacity and judicial checks may lead to draconian use of power by the regulator. [24] The search and seizure power under Section 66 allow the DPA to search and seize for up to 6 months a business's property on the basis of mere 'reasonable grounds' to believe that a business has violated or will violate the law. This is an excessive power that must be subject to judicial oversight in the same manner that other regulators such as the Competition Commission of India (CCI) require judicial sanction for search and seizure. There is also the possibility of conflict with other regulators, as some of the issues sought to be regulated by the DPA overlap with other existing frameworks. For instance, data portability may have a significant overlap with competition law.[25]
- There is also the issue of the technical and organisational capacity of the regulator, who in a mere 18 months, will be required to setup a nationwide infrastructure to monitor and enforce the entirety of the Bill. The relative nascency of the technology regulatory space in India, the lack of trained manpower to establish such a network of staff at scale and the parallel task of creating the codes of conduct mandated in the Draft Bill are all relevant hindrances. In a worst case scenario, organisations will have only six months to implement all the codes of practice in the Bill. All of this will place an unreasonable onus on data fiduciaries and processors to begin compliance with the Bill when such tangible regulatory uncertainty will exist in the system. Further, India's moves towards increasing its 'ease of business' rankings in the World Bank Index will also be significantly impacted by such draconian laws and regulations, primarily due to compliance and reporting costs.[26]

RECOMMENDATIONS:

a. *The overarching powers in favour of the DPA are excessive and unwarranted. The disproportionately broad powers vested in the DPA would effectively allow it to implement an entirely different framework of obligations for data fiduciaries and data processors by the simple act of issuing directions or codes of conduct without seeking submissions from industry representatives and other stakeholders and without following usual legislative processes. As a result, data fiduciaries and data processors will face significant uncertainty in managing their compliance with the law and this uncertainty will likely lead to inconsistencies and have a negative impact on data principals as a whole. We strongly recommend that the broad discretion of the DPA be replaced with transparent and clear provisions contained in the Bill or in implementing regulations that are passed in accordance with the legislative process.*

---

[23] Economic Impact Assessment of the Proposed European General Data Protection Regulation, Deloitte. Available at: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/about-deloitte/deloitte-uk-european-data-protection-tmt.pdf

[24] Suyash Rai, A Pragmatic Approach to Data Protection (9th February, 2018) available at https://blog.theleapjournal.org/2018/02/a-pragmatic-approach-to-data-protection.html

[25] *ibid*

[26] Ease of doing business: India aims to rank among top 30 countries, says Amitabh Kant, DNA. Available at: http://www.dnaindia.com/business/report-ease-of-doing-business-india-aims-to-rank-among-top-30-countries-says-amitabh-kant-2216007

b. *The independence of the DPA may be compromised by its dependence on the Government for finances in the form of grants (Clause 57) and appointment of chairperson and members (Clause 50(2)).*
c. *While the qualifications of the chairperson and members of the DPA include the need to have specialised knowledge of, and at least 10 years of professional experience in, relevant areas (Clause 50(4)), the Bill does not provide similar requirements for the appointment of its officers, employees, consultants and experts. A requirement to ensure that such officers also possess a similar level of qualifications will ensure that the DPA makes reasoned decisions based on a sound understanding of all relevant technical factors.*
d. *The Bill provides for a separate 'Adjudication Wing' of the DPA (Clause 68), whose Officers are required to be persons of ability, integrity and standing, and must have specialised knowledge of, and not less than seven years' professional experience in the fields of constitutional law, cyber and internet laws, information technology law and policy, data protection and related subjects. However, 'judicial experience' has not been mandated as a requisite qualification for such Officers, despite the fact that they make judicial determinations about the rights and liabilities of data principals and data fiduciaries, and whose orders/decisions are appealable to the Appellate Authority (Clause 84(2)).*
e. *The Bill empowers the DPA to specify the criteria on the basis of which rating in the form of a data trust score may be assigned to a data fiduciary (Clause 108(u)). Given the high implications of such score on an entity doing business in India, such criteria should be specified within the Bill itself. In the alternative, the criteria for determining data trust score may be specified by relevant industry bodies, who have the relevant experience to determine such factors.*

3. THE BILL'S HARSH PENALTIES AND CRIMINAL OFFENCES WILL PREVENT EFFECTIVE ENFORCEMENT

The Bill specifies a penalty up to INR 5 crore or 2% of total worldwide turnover of the preceding financial year whichever is higher, for infringement of the obligations to take prompt and appropriate action in response to a data security breach, to undertake a data protection impact assessment by a significant data fiduciary, to conduct a data audit by a significant data fiduciary, to appoint a data protection officer by a significant data fiduciary, and failure to register with the Authority as specified. For processing of PD, SPD and children's data in violation of the provisions of the Bill, failure to adhere to security safeguards and for transfer of personal data outside India in violation of the Bill, the prescribed penalty goes up to INR 15 crore or 4% of total worldwide turnover of the preceding financial year whichever is higher. (Clause 69). The Bill also specifies penalties for failure to comply with data principal requests without reasonable explanation, failure to furnish reports and returns as required, and for failure to comply with orders of the DPA. (Clauses 70-72)

Further, The Bill specifies non-bailable offenses for obtaining, disclosing, transferring, selling or offering to sell Personal Data / Sensitive Personal Data in contravention of the Bill, warranting imprisonment of up to 3/ 5 years respectively. Where an offence has been committed by a company, every person who, at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence, unless such person proves that the offence was committed without her knowledge or that she had exercised all due diligence to prevent the commission of such offence. If it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly. (Clauses 90-96)

- On the impact on excessive regulation which is overbroad rather than targeted, an NCSU study estimated that US federal regulations reduced economic growth by about 2% each year between 1949 and 2005.[27] According to the study, if federal regulations were still at levels seen in the year 1949, current (2013) GDP would be USD 38.8 trillion higher. A similar case can be seen in India's

[27] Federal Regulation and Aggregate Economic Growth, Journal of Economic Growth. Available at: https://link.springer.com/article/10.1007/s10887-013-9088-y

telecom sector, which is suffering from plummeting revenues.[28] In fact, it is increasingly accepted that the digital sector showcases the often-unnecessary top-down government intervention and regulation in light of private governance that is less voluminous, expensive or invasive. Ultimately the cost of all regulation percolates down to the consumer, the alternative of which would be for the regulated entity's profits to be eroded until it is no longer profitable or possible to remain in business – neither of which shall be considered the ideal result emanating from the Bill, as it would be counterproductive to user interest.

- Criminal penalties would certainly create a major disincentive for innovators and start-ups, keeping the principle of proportionality in mind. Most organizations in the internet ecosystem are very susceptible to reputational harm; and any news of an alleged involvement in a criminal offence, irrespective of whether such allegation is later proven true or not, would result in irreparable harm to the whole organization. Further, It is highly likely that the threat of criminal sanctions may incentivise entities to cover up data breaches or other violations of the Bill, thus denying opportunities of remedial action to those affected by a breach.
- Therefore, it is inappropriate to include worldwide turnover as a consideration in the levying of penalties for non-compliances under the proposed framework. Instead, the proposed draft should contain a fixed cap on penalties that may be levied and the same should be computed based on the articulated harm caused to an entity arising from such non-compliance. Such an approach would provide sufficient deterrent value for organisations while, at the same time, ensuring that entities are only penalised based on relevant considerations
- The Bill has also provided for criminal punishments. In past, we have witnessed the enforcement officials struggling without a proper understanding of the intermingling of law and technology. With harsh provisions contained in the Bill, and with a not so well-informed machinery, it will cause a great deal of discomfort amongst the companies handling personal data. It is possible that these provisions be enforced without a clear understanding of the technology and might lead to chaos. While several other jurisdictions have also prescribed criminal offences, making them cognizable and non-bailable is too strict

The penalties specified in the Bill are extremely high and appear to be unreasonable and arbitrary. The magnitude of penalties may stifle business and innovation for fear of penal sanctions. The law should not impose strict liability. However, organizations should be able to demonstrate that they have taken appropriate security and organizational measures to protect personal data in the circumstances.

Further in view of the restrictive data localisation provisions which in some cases of critical personal data will potentially implicate business activity limited to/in India, extending liability across total world-wide turnover and turnover of any Group entity of the data fiduciary which has no reasonable nexus to such "India only activity" will be unreasonable and arbitrary.

Further, these are calculated based on the 'total worldwide turnover' of the company, and not limited to the revenue generated in India or the actual harm that any non-compliance may have caused a data principal. Rather, a 'proportionate' approach would entail fixing a cap on penalties, which may be computed on the basis of actual harm caused due to any non-compliance. Reliance may be placed on existing jurisprudence in India in allied areas, such as Competition law, where the Supreme Court of India has limited the calculation of penalties in relation to the 'relevant turnover'.

The provisions related to imprisonment are draconian in nature and are not reflected in modern progressive data protection legislations such as the GDPR. They may be misused to unduly threaten senior management as well as ordinary employees of companies with personal liability.

[28] Avoid the temptation to overregulate telecom, Livemint. Available at: https://www.livemint.com/Opinion/7Pihq6ilqPqx8oqsLFbWZP/Avoid-the-temptation-to-overregulate-telecom.html

The Bill, in requiring data fiduciaries to demonstrate compliance, puts the burden of proof on the entity. This exposes companies to the threat of misuse, including baseless legal proceedings, including monetary and legal harm.

Implicating businesses and their management in legal proceedings would lead to a dip in the company's ability to carry out significant research and innovation activities leading a fall in the country's overall innovation abilities.

Imposing penalties (based on world-wide turnover) is applicable only to private bodies and businesses, and not to the Government. Given that the data protection law is intended to apply to both State and non-state actors as clearly mandated by the *Puttaswamy* privacy decision, adopting such a measure for calculation of penalties effectively penalises private businesses in a wholly arbitrary manner.

RECOMMENDATIONS:

- *In the interest of innovation and competition, it is of utmost essence that a framework of accountability through self and co-regulation be propagated via the DPA. Market propelled self-certification/ regulating mechanisms, along with incentivisation of voluntary disclosure schemes, could perhaps be an innovative way for the DPA to implement the codes of practice mentioned in the Bill. The industry can then voluntarily adopt global best practices and the DPA may retain the power to intervene only if it believes that there is a failure in market forces to act. Corporate practices, maturity, reputation and responsibility in addressing the concerns of the government and users should drive industry players to form a reliable and trustworthy ecosystem. Privacy principles and objectives could be broadly set out by the DPA on the basis of which data controllers should self-regulate and perform functions such as standard setting, development and implementation of codes, awareness generation and monitoring of their own compliances, audits etc.*
- *It is key that the DPA can discharge efficient independent regulatory oversight without the torturous annals of bureaucracy, red tape and lack of specific sectoral knowledge. The co-regulation model will help create an adequate implementation ecosystem – institutional capacities and capabilities, industry self-regulation, effective grievance redressal system, user awareness, active civil society, and research. The law should be outcome driven and focus on building the necessary ecosystem rather than just exclusively focusing on regulating data processing. This will ensure that deterrence and oversight does not disincentivize innovation and industrial growth across a wide range of sectors in India.*
- *The mechanism for determining penalties should be explicit, proportional and based on harm caused, and not the financial status of the data fiduciary. This is especially true for the distinction that the Bill makes for significant data fiduciaries, which are under far more onerous obligations. In determining the harm caused due to a violation, the diligence and security practices of the data fiduciary should be considered. In other words, entities that have been subject to data breaches and security attacks despite following best practices to secure their networks may be accorded relatively more lenient treatment, as opposed to entities with no internal processes and protections in place. The law should also consider that for responsible data controllers reputational harm (brand safety) would be as, if not more, important than financial harm. High penalties may not always be a deterrent and in fact may compel the suppression of violations due to perceived reputational harm.*
- *Compliances under various provisions of the Bill should be done on a self-compliance/self-declaration basis of late, such as employment law compliances for start-ups under the Start-Up Policy[29] of the*

[29] Labour Law Self Certification, Startup India. Available at: https://www.startupindia.gov.in/pdffile.php?title=Self-Certification&type=SelfCertifyCompliance&q=notification_Self_certificationformatsforcomplianceundertheLabourLaws.pdf&content_type=SelfCertifyCompliance

Government released last year itself. A similar approach should be taken by the Government in respect to impact assessments and audits as well, rather than mandating onerous external audits and reporting.

- *Gradually evolving the DPA's roles and responsibilities over time instead of overwhelming it with responsibility is the best way to ensure it can effectively fulfil its role. The DPA should focus on building a conducive ecosystem through digital literacy, awareness, providing guidance to start-ups and industry players etc. rather than taking on the role of a law-prescribing enforcement body. Further, in order to better prioritise the DPA's resources, reporting obligations should be limited highest risk issues instead of the current broad reporting mandates.*
- *Different sectors of the industry utilise different types of data and depending on their sensitivity, industry privacy practices are best developed specifically for such sector. With legal recognition of self-regulation this can be achieved with self-regulatory organisations defining the process and codes of practice. Such an approach also marks continuity from the existing framework, under Rules 8(3) and 8(4) of the IT Act, Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011.*
- *Checks and balances should be imposed on the functioning of the DPA by prescribing due process within the Bill, along with requiring heightened independence and transparency in its functioning.*[30] *Due process to be followed by the DPA may include expressly providing the parameters that need to be considered by the DPA for discharging any statutory function within the Bill, including imposing penalties. Ensuring there are rigorous standards for the officers and Chairman of the DPA will increase both the credibility of the organisation as well as ensure effective enforcement of the Bill.*

4. DEFINITIONS IN NEED OF REVIEW

SENSITIVE DATA

The expansion (from the current regulatory regime) of the definition of sensitive personal data (SPD), coupled with the absence of an exception for data made manifestly public by the data principal, appears to make the Bill extremely prescriptive. The list of SPD in the Bill is very wide which will lead to compliance challenges for businesses and will strongly discourage innovation. For example, there is no guidance on what qualifies as data revealing caste/religious/political beliefs - even surnames that reveal caste can be considered SPD under current list which leads to various impractical implications. The aforesaid information is generally freely available or accessible in public domain and hence it should not be regarded as sensitive personal data or information for the purposes of this Bill. Similarly, what qualifies as "behavioral characteristics of a data principal" under the definition of biometric data - this could impact functions dependent on data analytics of behavioral patterns; for example: assistive technologies by people with disabilities. The lack of infrastructure, time, and money with most startups, who will need to operationalise higher levels of protection for all potential SPD, will also inhibit entrepreneurship. The guiding principles to determine SPD can be used to include any type of data to this category of personal data. SPD categorisation can provide a higher-level protection to possible harms arising from discrimination and profiling based on identities. Passwords and financial data do not fall in this category. Globally, around 68 countries have a comprehensive data protection regime, but none have included passwords or financial data as SPD. Globally, there is no category of critical

[30] supra note 22

personal data being defined or identified. Any requirement to further categorise the critical personal data will only increase the complexity of the data protection regime and should be avoided.

RECOMMENDATION:

Unlawful processing of SPD should invite higher penalties, as opposed to additional safeguards. Safeguards, by their very nature, are best identified by industry through contextual self-regulation and assessment of harms. Therefore, instead of regulatory prescription, the law may consider (a) requiring higher threshold of processing (without prescription of what constitutes higher security and protection, (b) explicit consent, and (c) increased penalties. Penalisation should be intrinsically linked with the harm done, diligence observed, best practices were followed and remedial measures taken by the processor. The Bill should also include a clearer definition of what processing of SPD would be, i.e. explicit collection and processing of specific categories of data and not merely potential inference of SPD. The list of SPD data should also be shortened for ease of compliance - even the GDPR, which are widely regarded as one of the most comprehensive data protection laws of our time, has a narrower list of SPD than the current Bill.

BIOMETRIC DATA

Biometric data has been incorporated in the definition of sensitive personal data which receives a higher degree of protection. While this is a rational and prudential move, the definition of biometric data as it exists is overbroad and can lead to unintended consequences. For instance, the definition as it exists is overbroad and extends to any photograph containing any identifiable individual. This severely limits the common, non-sensitive use of photographs that contain a facial image.

RECOMMENDATION

Thus, it is recommended that a clause be added to clarify that data is only considered biometric when it is used for the identification of an individual. Moreover, it must be clarified that photographs of individuals and the data derived from them are outside the scope of biometric data.

5. NOTIFICATION REQUIREMENTS AND PURPOSE LIMITATION

The Bill incorporates certain 'principles' for processing of personal data, such as 'collection limitation' on the basis of data that is *necessary* for processing (Clause 6) and 'purpose limitation' in that 'personal data shall be processed only for purposes specified or for any other incidental purpose that the data principal would *reasonably expect* the personal data to be used for, having regard to the specified purposes, and the *context and circumstances* in which the personal data was collected. (Clause 5). (emphasis supplied)

The Bill also provides stringent criteria for the provision of notice to the data principal while collecting data, and the content of such notice. (Clause 8). It burdens data fiduciaries with the obligation to ensure that personal data processed is complete, accurate, not misleading and updated, having regard to the purposes for which it is processed. (Clause 9). Further, the data fiduciary may retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed and must undertake periodic review in order to determine whether it is necessary to retain the personal data in its possession.

While the provision of effective notice is an important and meaningful pre-requisite to the processing of a data principal's personal data to ensure consent, the manner in which the proposed framework prescribes that a notice must state all individuals or entities including data fiduciaries and data processors with whom such data may be shared is burdensome without concomitant benefits. This is likely to lead to notice fatigue given the sheer number of notices a data principal will receive, leading in turn to ineffective communication of notice.

This is a highly restrictive approach that burdens the data fiduciary with an unwelcome and undesirable (burden of) interpretation as well as compliance based on vague, broad and inherently subjective terms. The Bill does not provide any specific guidance for the interpretation of these criteria. Vague and ambiguous statutory language will result not only in the objective of the Bill or enactment being open to subversion but also lead to contradictory interpretations increasing avoidable business risk and exposure and consequent litigation.

Mandating such broad criteria is likely to compromise numerous business models which have contributed to making the internet a domain for knowledge-sharing and commerce, as it puts them on the defensive for taking subjective calls on processing.

From a user perspective as well, foisting upon the data fiduciary the duty to "take calls" regarding the interpretation of these terms deprives the user from exercising direct agency over the circumstances in which she would want her data to be processed.

Given that (clear, free, informed, specific) 'consent' (also capable of being withdrawn) is the primary ground for processing of data which gives primacy to the user to determine when her data should be processed, this provides adequate legal basis and consequently there is no further requirement for a regulatory framework allowing for subjective determinations to be made regarding processing.

These regulatory restrictions would negate the growing role of Big Data processing as well as Government initiatives under Digital India which rely on processing large amounts of data for service delivery and public interest.

RECOMMENDATIONS:

a. *The above requirements should be applicable on a "best endeavour" basis rather than in the nature of an absolute obligation.*
b. *Notice should only be required to contain categories of individuals or entities with whom data may be shared without any loss of protection.*
c. *As per Clause 11, the data fiduciary must be able to demonstrate that any processing undertaken by it or on its behalf is in accordance with the provisions of the Bill. Whilst the intent of this Clause is accountability, we suggest the specific reference to risk-based approach is brought in the Act, a similar approach is present in the Article 24 (1) of the GDPR[31]. While the record-keeping obligation under Clause 34 may be used to demonstrate compliance, Clause 34 (2) provides that the data fiduciary shall maintain records "in such form as specified by the authority". This specifically restricts the flexibility of organisations to devise their own compliant forms of record keeping. Given that the law shall be applicable equally to all it shall be unfair to have one common standard imposed by the DPA. Instead, records should be kept in a manner that allows them to be produced to the DPA on request, consistent with Clause 11(2). But the manner of form of records should be left to the discretion of the data fiduciary. We therefore recommend deleting this section.*

6. PRIVACY BY DESIGN

[31] See Article 24(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Data fiduciaries are mandated, under Clause 29 of the Bill, to implement policies and measures to ensure 'privacy by design' which draws from Article 25 of the GDPR (data protection by design and by default). The privacy by design obligations in the Bill involve designing managerial, organisational, business practices and technical systems in a manner to anticipate, identify and avoid harm to the data principal, implementing policies and measures to ensure that fiduciary obligations are embedded in the organisational and business practices of the Company, ensuring that any innovation is achieved without compromising privacy interests which must be protected throughout processing from the point of collection to deletion of personal data, ensuring that processing of personal data is carried out in a transparent manner and that the interest of the data principal is accounted for at every stage of processing of personal data. The language of the provision makes it difficult to translate the theoretical principle of "privacy by design" into concrete implementable obligations. In addition, unlike the GDPR, the Bill creates an absolute obligation and unlike the GDPR does not recognize that this obligation ought to balance the rights of data principals with the costs of implementing privacy measures.. In particular, the GDPR allows the controller to take into account the costs of implementation and allows the controller to determine measures that are "appropriate" in the relevant circumstances. In effect, the GDPR is far less prescriptive than the Bill in this regard.

RECOMMENDATIONS

The "privacy by design" obligation should be amended to not be an absolute obligation but rather to allow a data fiduciary to implement measures that it determines to be appropriate having regard to the cost of implementation and the risks to the rights and freedoms of data principals including the likelihood and potential severity of these risks based on the nature, scope and purposes for which it processes personal data. We also strongly recommend the measures listed in the Bill to be less prescriptive and instead set out principles that each data fiduciary should consider in its organisation and business practices.

7. DATA BREACH NOTIFICATION

Clause 32 of the Bill imposes an obligation on data fiduciaries to notify the Authority and data principal if there is a personal data breach. A notifiable personal data breach is one which is "likely to cause harm". This threshold is lower than the threshold adopted in the GDPR. Unlike the GDPR, there is no express requirement for the data fiduciary to have knowledge of the data breach in order for the obligation for notification to be triggered. This is particularly problematic and out of step with data breach notification regimes elsewhere in the world. The Bill also implies in Clause 61 that the Authority has the power to issue codes of practice covering actions to be taken by data processors if there is a personal data breach.

RECOMMENDATIONS

a. *The data fiduciary's obligation to notify should be amended in line with GDPR to only be triggered if the data fiduciary has actual knowledge of a notifiable data breach as it is impractical for this obligation to be triggered even before a data fiduciary becomes aware of the breach. The threshold for notification should also be revised to be consistent with GDPR and include exceptions where notification is not required.*
b. *We strongly recommend that the Bill include a period of time allowing for data fiduciaries to investigate potential data breaches before their notification obligation is triggered as this would ensure that both the Authority and data fiduciaries are not administratively overburdened by notifications of possible breaches that may not have an actual, material impact on the rights of data principals. This is also consistent with international practice, for example the Australian mandatory personal data breach notification regime.*
c. *The Bill should set out more transparently when data principals are required to be notified instead of leaving this to the Authority's discretion, and the Bill should include appropriate exceptions. For example, GDPR requires this when "there is a high risk to the rights and freedoms of natural persons", along with a set of transparent exceptions such as if the controller has implemented appropriate technical and organizational measures, or taken subsequent actions or if individual notification would involve disproportionate effort. By including these notification parameters clearly and transparently in the Bill, instead of leaving them to the discretion of the Authority, will ensure that data fiduciaries have a clear*

understanding of their obligations and are incentivised to act quickly and appropriately to address data breaches.

8. GROUNDS OF PROCESSING

Another issue on which the framing of the current Draft Bill may be reconsidered is that of the grounds upon which personal data may be processed. Under the current Draft, Chapter III details the various grounds on which the processing of personal data may be carried out by a Data Fiduciary. These include consent, Government purposes, compliance with court order, employment purposes, and other reasonable purposes to be notified. While these grounds are all valid grounds of processing personal data, there is a notable omission of processing for the purposes of contract (or 'contractual necessity'). This ground is important in the modern data economy to prevent disruption of goods and services by the need to repeatedly procure consent for processing from users. Under this ground, where a user enters into a contract, the Data Fiduciary may process data as may be required or relevant for purposes of the contract. An important aspect of user autonomy is the freedom to enter into contracts and agreements as they see fit. Various legal aspects of such agreements are governed by the Indian Contract Act, 1872 which addresses various issues such as offer, acceptance, validity, and consent. Within this context, the lack of inclusion of contractual necessity for personal data processing is surprising and significantly out of step with global best practices contained in foreign frameworks. Retaining such an approach will complicate business, result in consent fatigue for users, and disrupt the online economy – while at the same time undermining user autonomy to enter into contracts as they see fit.

Further, the ground of "reasonable purpose" is to be determined by the DPA instead of being left to an assessment of the data fiduciary. The absence of such a ground significantly complicates the conduct of business online – without addressing a countervailing harm or perceived harm.

RECOMMENDATION

The Ministry should consider including a specific provision in Chapters III and IV permitting data processing on the grounds of contractual necessity. This may be phrased in the following language: "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract."

Further, the ground of "reasonable purpose" should not be determined by the DPA, but left to be determined by the data fiduciary in line with the "legitimate interest" ground in GDPR. We recommend addition of language as follows: "processing is necessary for the purposes of the legitimate interests pursued by the data fiduciary, except where such interests are overridden by the interests or fundamental rights and freedoms of the data principal which require protection of personal data." We also recommend extending this ground to the processing of sensitive personal data.

9. PROCESSING DATA OF CHILDREN

The Bill sets 18 years as the age of obtaining independent consent, making every individual below the age of 18 a child within the framework of the Bill. Processing of a child's personal and sensitive personal data requires that the data fiduciary protect the child's rights and interests. Verification requirements pose an insurmountable logistical challenge, especially over the internet, where users are invisible. Additionally, in order to conduct the verification, the mechanism and process may require the child to share official documentation to evidence her age. If she is a child, i.e. under the age of 18 years, gathering this data itself, in a certain set of circumstances, may not be possible for data fiduciaries without running afoul of the verification provision in the Bill. Additionally, guardian fiduciaries, despite their very nature of inviting internet traffic from children, are precluded from targeting services to them. This is problematic, because it may be considered unfair to restrict a child-user's access to seamless and personally tailored user experience purely by virtue of them being under 18 years of age and also for a guardian fiduciary being placed in a more restrictive position compared to any other data fiduciary (which is not the case under equivalent laws such as GDPR). It is pertinent to note that even extant statutes that prescribe age-based criteria for access of certain content, do not lay down any requirement for verification of age.

It is also to be appreciated that the Bill acknowledges that the role of a notified guardian data fiduciary exclusively offering counselling or child protection services is overwhelming and does not require parental consent for processing of personal data of children.

RECOMMENDATION

The digital age of consent for children should be lower than the contractual age and can be further grouped as between below 13 years (consent by parents or legal guardians), 13 - 18 years (or possibly 16 years – with parental consent) and above 18 (consent of the user is sufficient) which is consistent with international laws. Further, it may be useful to link age and consent requirements with due diligence on the part of the data fiduciary, as opposed to verification mechanisms. So long as the entity exercises care and caution in seeking age-based confirmations from the user, the entity must not be held liable for misrepresentation of age by the user and use of data collected thereof. To ensure the protection of child-users, it may be useful to embody an approach of notice and consent from the child-user, along with parental participation and robust awareness programmes that help the child-user understand the ramifications of her access to the services and sharing of her information. This composite approach may confirm that the entity has conducted its due diligence, and therefore accord safe harbour from liability associated with processing the child-user's data.

10. CONSENT FOR MINORS

Where children's data is processed by data fiduciaries, the Bill imposes special requirements to incorporate 'appropriate' mechanisms for age verification and parental consent. The Bill also creates a category of 'guardian data fiduciaries', as notified by the DPA where a data fiduciary operates commercial websites or online services directed at children or processes large volumes of personal data of children. (Clause 23). Guardian data fiduciaries are barred from profiling, tracking, or behavioural monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child. 'Child' is defined under the Bill as a data principal below the age of 18 years (Clause 2(9)).

These measures may result in excluding a large swathe of the Indian youth population, which forms a bulk of internet users, from participating in the digital economy.

Given the onerous burden of compliance to these provisions, several businesses may choose to opt out of providing child-focussed services and services targeted to any users suspected to be below 18 years of age as also this will negatively impact any business which includes the possibility of participation by persons below the age of 18 years. This will preclude access to valuable sources of learning and communication for a large part of the population that would otherwise stand to gain from such access.

It is also pertinent to note that while the definition of child as a person below 18 years has been retained in the Bill in deference to the age of consent for contract as per the Indian Contract Act, 1872 read with the Indian Majority Act, 1875, the Committee has explicitly acknowledged that *"from the perspective of the full, autonomous development of the child, the age of 18 may appear too high."* (Page 44 of the Report) recognising that mandating 18 years will not be reasonable in light of the varied nature of online activity. This is also in line with the observations of the Delhi High Court in the case *K.N. Govindacharya v. Union of India* [W.P. (C) 3672/2012] where the Court recognised the general practice of mandating 13 years as the lower (age) limit in the case of social media. Additionally, EU GDPR Article 8, requires parental consent for children below age of 16 years, allowing member states to provide by law a lower age for consent, provided it is not below 13 years.

RECOMMENDATIONS

It is thus recommended that the Bill not mandate an age limit of 18 years in the data protection law, leaving it to be interpreted based on the context of such activity. Alternatively, a 'carve-out' could be effectuated from the age of majority legislation for purposes of personal data processing of children between the ages of 13 years and above, in tune with principled considerations around the object of processing as is done in most data protection legislations around the world. Such a carve-out would be additionally supported by the overriding effect of the data protection law over any inconsistency vis-à-vis with the provisions of any other law as mandated by Clause 110 of the Bill.

11. DATA STORAGE LIMITATION

The Draft Bill limits data fiduciaries' ability to retain personal data of a principal beyond the period required to deliver services to them. Exceptions to this requirement are very limited and include compliance with other legal obligations. Mandating the deletion of data pertaining to the data principal restricts the ability of the fiduciary to perform important tasks that enable the improvement of the quality of services offered.

RECOMMENDATIONS

The need to undertake these processes after the initial purpose of data collection has been fulfilled can be balanced by the need to minimize privacy risks by allowing data fiduciaries to retain data in a de-identified form, thereby minimizing the risks attendant. This will allow fiduciaries to carry out the processes required to improve upon their services while adequately protection the privacy of data principals.

12. UNCLEAR TRANSPARENCY AND ACCOUNTABILITY MEASURES

In Chapter VII, the Draft Bill prescribes various transparency and accountability measures for data fiduciaries to implement. While we applaud these measures, we urge the Ministry to re-evaluate each of these measures to provide additional clarity on the specific compliances required to be undertaken. For instance, Section 29 of the Draft Bill requires data fiduciaries to implement policies to ensure Privacy by Design. While several of these measures are clear, many do not provide any indication of what compliance is required. For instance, clause (g) provides that "*the interest of the data principal is accounted for at every stage of processing of personal data".* However, it is unclear how this is to be implemented in practice. Requirement of security safeguards have been made under Section 31, which also extends to data processors.

Similarly, data principals are required to be informed of 'important operations' 'periodically' with regard to processing of personal data. However, these terms themselves have not been defined, thus leading to lack of clarity about what operations qualify and how periodic such notice must be (leading to risks of notice fatigue). compliance more specific legislative drafting approach is recommended for effective and meaningful compliance.

RECOMMENDATIONS

Therefore, we urge the Ministry to rationalise the obligations contained in this Clause by either prescribing a safe-harbour for entities implementing efforts to a 'reasonable' level, or further clarify the obligations contained under these and other provisions of Chapter VII.

13. ANONYMISATION

The proposed framework has recognised the value of anonymisation as a technical process to secure personal data. It has exempted anonymised data from restrictions that are placed on the processing of personal data. However, the standard of anonymisation prescribed in the Draft Bill is onerous and impractical. This standard requires personal data to be 'irreversibly' anonymised in order to qualify for the proposed exemption. Given the constant development of technology, to anonymise data to an irreversible degree is technologically impossible.

Further, the DPA may not have adequate capacity to provide adaptable standards across industries. Therefore, data fiduciaries should be allowed to establish standards based on industry best practices that will evolve with time.

RECOMMENDATIONS

Therefore, it is recommended that the standard of anonymisation be rationalised, changing it from 'irreversibility' to a level of anonymisation where 'a data principal cannot reasonably be identified.'

14. PROCESSING FOR RESEARCH, ARCHIVING OR STATISTICAL PURPOSES

The proposed framework has recognised the value of data processing for research, archiving or statistical purposes, which enable innovation and advancement of issues in public interest, leading to aggregate welfare. However, the requirement of a case-by-case determination of whether research purposes are permissible would lead to a significant backlog and substantial delays that would in turn prove to be a hurdle in completion of useful research.

RECOMMENDATIONS

In order to strike a balance between protecting privacy and ensuring the continued development of important initiatives, data fiduciaries should be allowed to make a determination about whether processing fits these purposes to allow for greater flexibility.

15. PROHIBITION ON RE-IDENTIFICATION

The Draft Bill, in a prudent move, prohibits the non-consensual re-identification of personal data. This is an important protection that secures the privacy of data principals. While creating a data protection framework, it

is important to align incentives with privacy friendly actions taken by data fiduciaries. It becomes even more vital to ensure that legislation does not lead to unintended or unforeseen consequences such as requiring the data fiduciaries to take privacy unfriendly steps.

RECOMMENDATIONS

Thus, it is important to add a provision to the Draft Bill to clarify that compliance with any provision of the Bill will not be interpreted to require a data fiduciary to re-identify data that has been de-identified or otherwise not directly identifying a data principal.

16. APPLICABILITY

The Draft Bill seeks to claim a very broad extra-territorial reach through Section 2. While the ostensible purpose is to extend protection to as broad a swathe of Indian citizens as possible, the Bill in its current form is likely to lead to situations of conflict of laws. In particular, where there are established contractual relationships between data principal and data fiduciaries who have already agreed to certain protections subject to the laws of the jurisdiction in which the data fiduciary is present, this overbroad extension of reach negates the freedom to contract and the validity of choice of law.

RECOMMENDATIONS

Thus, the Bill should not be applicable to processing of personal data that is pursuant to an agreement between data principal and data fiduciary subject to laws of another jurisdiction.

17. SIGNIFICANT DATA FIDUCIARIES

The Draft Bill, in its current form, also creates a differential system of regulation for larger entities engaged in data processing activities – such as significant data fiduciaries, and guardian data fiduciaries (in relation to child data). However, instead of focussing on concepts such as harm and risk, the criteria also take into account factors such as volume of data processing, turnover, and deployment of new technologies. In other words, entities which undertake innovation and deploy new technology are penalised by the imposition of additional compliance requirements. The significant data fiduciaries are subjected to registration with the DPA, and will also be subject to higher penalties for any violations. Classification of data fiduciaries might not be subjected to a desirable standard of transparency, and the Bill also does not provide recourse for the data fiduciary to contest their classification. This might become a contentious issue.

Such an approach causes serious harm to India's ambitions to emerge as a hub of innovation and technology. Instead, the proposed framework should aim to incentivise and to facilitate to the maximum extent possible and only intervene where articulated harm to any specific party results.

RECOMMENDATIONS

Therefore, we urge the Ministry to review this application to classification. We would urge that a uniform approach to compliance be observed – with scope for intervention by the regulator only in cases where articulated harm results.

18. DATA PROTECTION OBLIGATIONS ON SIGNIFICANT DATA FIDUCIARIES

The Bill creates different obligations for entities who are notified by the DPA in its discretion as 'significant data fiduciaries', having regard to factors such as volume and sensitivity of personal data processed, turnover, use of new technologies and all other entities (Clause 38). Certain key data protection obligations, such as DP Impact Assessments, Record Keeping obligations, Data Audits, and appointment of a Data Protection Officer, will apply to significant data fiduciaries. However, the language in the Bill should be clarified to indicate whether those obligations *only* apply to significant data fiduciaries. In addition, the DPA should not have the discretion to determine to whom these obligations should apply. This should be set out transparently in the Bill itself. For example, in Article 30 of the GDPR there is an exemption from certain record keeping obligations for organizations that have less than 250 employees unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences. The GDPR contains objective criteria, rather than granting the data protection authority broad discretion to determine to whom this obligation applies.

RECOMMENDATIONS:

a. *The Bill seeks to makean arbitrary distinction between data fiduciaries and 'significant data fiduciaries' and subject them to discriminatory obligations and liabilities. The pith and substance of the data privacy law is intended to protect the citizen's privacy (which is a fundamental right), and from this sole and overarching perspective, both large and small data fiduciaries are equal. Thus, making this distinction based on the size of entities and/or other irrelevant factors would amount to discrimination without a rational nexus with the objective sought to be achieved. The bill should consider removing this distinction. In the alternate, it must specify the categories for creating distinctions in a way that is more clearly linked to the potential for harm, and not base it upon irrelevant considerations.*
b. *This category is likely to include all entities which undertake innovation and deploy new technology, and unduly burden them by the imposition of additional compliance requirements, in addition to discouraging innovation in the digital economy.*
c. *Data obligations should be imposed on entities based on articulated harm to any specific parties, instead of indirectly penalising innovative businesses. The latter approach would harm India's ability to emerge as a hub of innovation and technology.*

19. EXTRA-TERRITORIALITY

The Bill applies to data processors and data fiduciaries established outside of India if the processing is:

- In connection with any business carried on in India; or
- systematic offering of goods and services to Data Principals in India; or
- any activity which involves profiling of Data Principals within India.

RECOMMENDATIONS

a) *For clarification and to ensure that this extra-territoriality is consistent with GDPR, the third limb should be qualified with "as far as the profiling is with respect to the data principal's activities within India".*
b) *Moreover, the Bill should clarify whether the Bill is intended to apply to data processors established in India that are processing personal data of non-Indian individuals under a contract with a non-Indian data fiduciary as Clause 104 of the Bill implies that the scope of the Bill covers this scenario unless the Central Government grants an exception.*

This reflects the considered position of Broadband India Forum and represents the view of the majority of its membership.

BIF
Broadband India Forum