The Dialogue™
INFORM ENGAGE IDEATE

IMPACT STUDY:
PERSONAL DATA PROTECTION BILL ON THE START-UP ECOSYSTEM

TABLE OF CONTENTS

TABLE OF ABBREVIATIONS

COVID 19	SARS-CoV-2 Coronavirus 2019
DPA	Data Protection Authority
EU	European Union
GDPR	General Data Protection Regulations
IP Address	Internet Protocol Address
IPR	Intellectual Property Rights
JPC	Joint Parliamentary Committee
MSMEs	Micro, Small & Medium Enterprises
NASSCOM	National Association of Software and Service Companies
PDP 2019	Personal Data Protection Bill 2019
RBI	Reserve Bank of India
SMB	Small & Medium sized Businesses
SMEs	Small and Medium Enterprises
TRAI	Telecom Regulatory Authority of India
UK	United Kingdom
USA	United States of America
VC	Venture Capitalist

ACKNOWLEDGEMENT

The Dialogue's research team would like to express our deep gratitude to Saikat Datta, our Strategic Advisor, for his patient guidance, enthusiastic encouragement, and useful critique of this report . The authors would also like to thank Shefali Mehta for her assistance in providing inputs. The team would also like to extend our thanks to the participants of our focus group discussions for offering us their time and resources in collecting inputs for the report. We are grateful to Bhavya Birla for his research assistance on this report. Finally, we wish to thank Abhinav Kashyap for working as a designer for the cover and layout of this report. .

We also express our sincere thanks to Kazim Rizvi, Founding Director of the Dialogue for his guidance throughout the project and for his inputs on multiple drafts of this report.

ABOUT THE AUTHORS

Arya Tripathy is Partner at PSA (Priti Suri and Associates)

Karthik Venkatesh is the Research Coordinator at The Dialogue. His interests lie in the intersection of Data Governance and regulation of emerging tech. At the Dialogue, he heads the research efforts on Non Personal Data Regulations and leveraging data for effecting societal change.

Trisha Pande is the Policy Manager at The Dialogue. She is interested in the intersection between technology and development studies. At The Dialogue, she works on a range of policy issues to make the internet a safer space for all. She currently leads research on gender and technology.

*These names have been arranged alphabetically

METHODOLOGY

The Dialogue conducted a series of five stakeholder consultations with startups, researchers, law firms, and consulting organisations in 2020. These stakeholder consultations helped garner insights from members of the start-up and SME community in terms of their initial sentiments of the PDP Bill 2019. There were a number of experts invited for the events, which were part of The Dialogue's network on issues related to data protection and compliance.

The experts were from legal, policy and technical fields, and have significant experience in understanding regulatory issues faced by the start-up and SMB community.

There were blockchain experts, CTOs of B2B SaaS companies and co-founders of social enterprise, data-driven start-ups which The Dialogue managed to engage. The participants of the stakeholder consultations came from diverse backgrounds, and are solving equally important but vastly different problems through their business models.

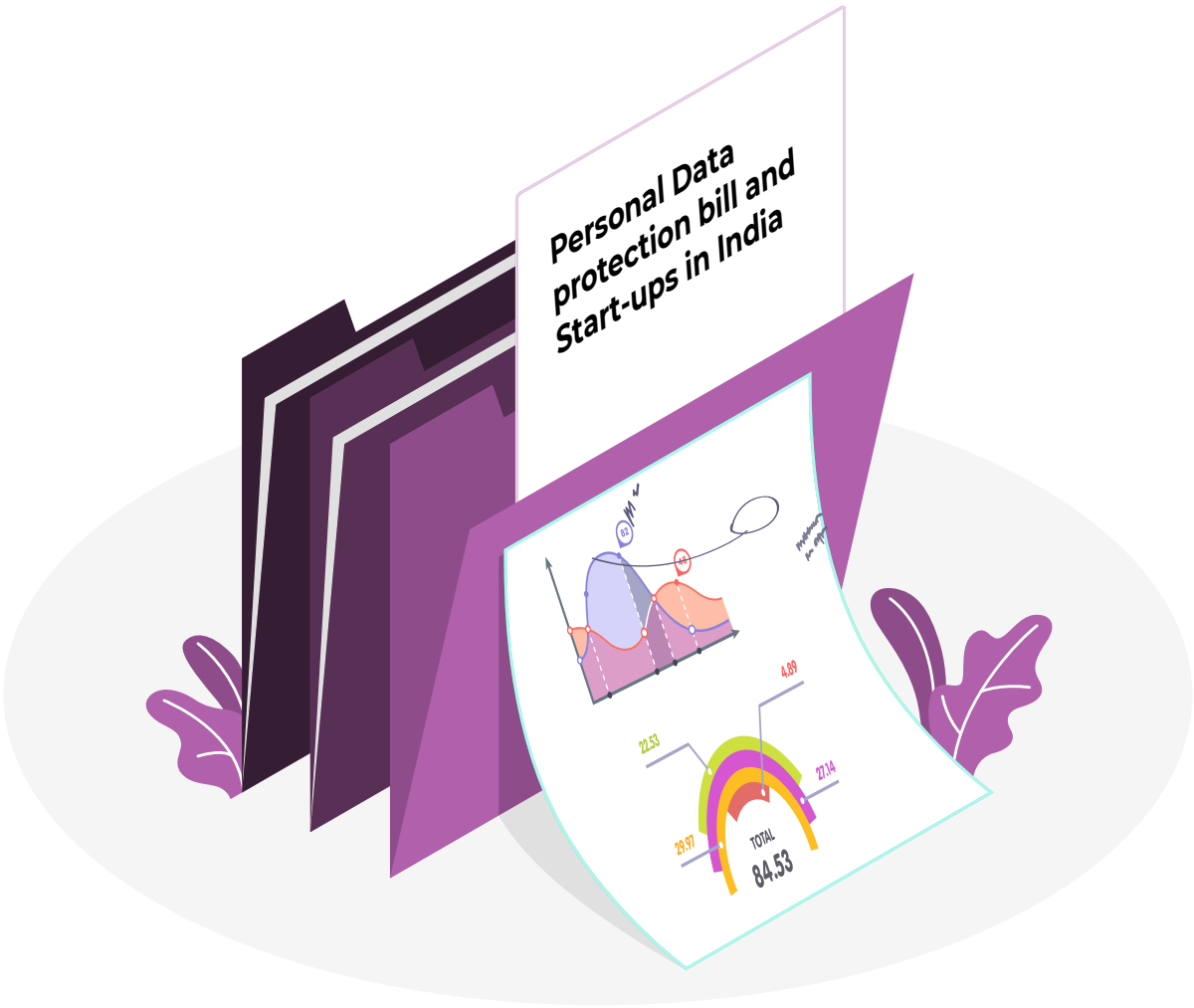
This report is a unique effort by The Dialogue to understand the startup ecosystem with respect to personal data protection in India. It has original analysis conducted by the team at The Dialogue, by combining inputs collected over the course of 2020 from startups, with existing literature that was reviewed throughout the process.

NUMBER OF START-UPS AND TOP TWO AREAS

The Dialogue engaged with **57 start-ups** in the course of the 5 stakeholder consultations.

These start-ups belonged primarily to the digital services sector - comprising members from the cryptocurrency, cloud computing, food delivery, data analytics, invoice management, website management, and software development space.
The Dialogue also witnessed remarkable presence from the social enterprise/policy sector. Representing start-ups invested in solving problems centred around urban governance, data collection and technological research, social mobilization, consumer trust, internet commerce ecosystem and architecting social transformational interventions and campaigns using technology to create positive impact.

EXECUTIVE SUMMARY



EXECUTIVE SUMMARY

The Dialogue organised a series of **5 stakeholder consultations** across the months of starting from March till October on *'The Need for a Progressive Data Regulation Regime for Indian Startups'*. The Dialogue invited **57 startups**, from sectors cutting across health, education, social enterprise, cloud computing, software development, data analytics, fintech, marketing, business consulting and accounting.
In addition to this, The Dialogue invited legal experts from firms which deal with a start-up clientele such as PSA and Ikigai Law.

2021 is currently marked with a total number of 490+ Unicorn companies globally, out of which 25+ are in India, contributing to India's status as the third largest start-up ecosystem - only behind China and the USA. What changed from 2017 to 2018 for India was the addition of new and specialised sectors (ed tech, food delivery, B2B, healthtech, insurtech etc.), even as the stronghold of already thriving internet software & services - e-commerce & marketplace and fintech, only increased. While the pre-2018 Unicorns largely belonged to the sectors of internet software & services, e-commerce and marketplace and internet retail, the future is data-driven and India has emerged over the years as a fast and capable innovator and adapting to newer technologies.[1]

The Indian start-up ecosystem has evolved, driven by factors such as growth in number of funds/angels, evolving technology, higher smartphone and social media penetration, growth in incubators and accelerators, younger demographics, etc. A large contribution to this growth trajectory comes from the government's initiatives in easing foreign investment, enabling policies and programs in the form of **Start-up India** and **Make in India**, and incubating start-ups.

The COVID-19 pandemic has affected economies across the globe, requiring governments to prioritize survival over innovation, at least for the time being. While the pandemic may be temporary, the policy decisions and legal framework that government implements will have lasting effects. With personal data forming building blocks of tech enabled businesses and informational privacy being recognized by the Hon'ble Supreme Court as a fundamental right, a dedicated and holistic data protection and privacy regime is therefore imperative. The proposed **Personal Data Protection Bill, 2019,** when enacted, will be India's maiden data protection law and will impact all companies in unprecedented ways, specifically having far reaching consequences for the Indian start-up ecosystem. While the need and urgency for a robust data protection regime is well perceived, it is equally essential that a pragmatic approach is adopted, where specific requirements of start-ups and early growth companies is taken into account. This calls for the need for the government to engage with the start-up ecosystem players in order to factor their concerns as they finalise and enact the law.

The vagueness in definitions and clarity as to what constitutes categories of sensitive personal data, personal data and non-personal data might pose a significant challenge to startups in India. While there is expected to be a separate set of guidelines to regulate non-personal data in the future, the PDP 2019 already mentions what non-personal data is ("the data other than personal data"), and indicates that the Central Government would be empowered to gain access to this data. Further, there is the necessity of a detailed timeline in terms of PDP 2019's implementation.

[1] PTI (2021, Jan.6) India 3rd largest startup ecosystem; home to 21 unicorns: Ambassador to US, Business Today, accessible from https://www.businesstoday.in/current/economy-politics/india-3rd-largest-startup-ecosystem-home-to-21-unicorns-ambassador-to-us/story/427132.html

Start-ups will hugely benefit if they have greater clarity on compliance timelines and the procedures for the same. Going forward, this will be a significant area for start-ups as they engage with the text of the PDP 2019.

The creation of a regulatory sandbox to exempt start-ups from heavy compliances is envisaged in the PDP Bill 2019. Leeway is provided for start-ups to innovate and exemptions are provided for purpose limitation, data minimisation etc., to provide the companies to work on sectors that pertain to AI, machine learning or other emerging technology for public interest. This could be an experimental solution to reduce compliance burden on start-ups with innovative solutions for societal needs - although the Data Protection Authority will have to carefully define criteria so as not to exclude those startups which might need the regulatory sandbox umbrella.

Some of the ways that PDP 2019 might impact the start-up ecosystem are highlighted below: -

A) STEEP COMPLIANCES: During a merger/acquisition, if the investor or the target company are data fiduciaries, there is a possibility that they may qualify as "significant data fiduciaries". This will be based on certain criteria, such as sensitivity of data processed and its volume. PDP 2019 mandates significant data fiduciaries to obtain registration, conduct independent audits, and comply with reporting requirements. This is likely to increase compliance costs for start-ups, which may not commensurate with their available resources and funds.

B) RESTRICTIONS ON CROSS BORDER DATA FLOWS AND DATA LOCALISATION: PDP 2019 provides for strict cross-border data flow restrictions, which may limit the ability of Indian start-ups to access cost effective technology and storage solutions such as cloud services and foreign data centers that operate globally. For young start-ups, minimising operating costs is essential. Where the cross-border restrictions remain as is, start-ups will be required to incur substantial costs in either complying with such data transfer requirements, or for storing and processing data within India . Consequently, cost of operations will increase, which may impede their ability to develop and deliver goods and services.

Alongside data transfer restrictions, PDP 2019 continues to retain provisions for data localisation. These compliances force companies in two ways. Firstly, setting up domestic processing and storage capacity is not feasible without an upfront cost. Secondly, data migration efforts for bringing back processing infrastructure would further impose costs. In addition to extra capital investment, compliance to new regulations may make their business model unprofitable, putting them in a situation where they have to reassess expansion plans, or shop for other jurisdictions.

C) STIFLING INTELLECTUAL PROPERTY RIGHTS: PDP 2019 under Clause 91 gives government access to anonymised personal data or non-personal data of any company as they may deem fit, for planning and policy purposes. Without adequate checks and balances, the possibility of infringement of third party intellectual property and similar rights cannot be ruled out, and where such a situation arises, it is likely to discourage innovations, and inventions. However, the revised report from the Committee of Experts on Non Personal Data Governance Framework has recommended the deletion of the clause. We welcome such a move and hope that the same is reflected in the new draft of the PDP Bill, which was arrived at after deliberations by the JPC.

As an integral stakeholder in the digital ecosystem, conversations regarding data governance must have representations from the community as well. The need for this exploration and enquiry began because of the uncertainty faced by startups during the COVID-19 crisis coupled with the changing data governance landscape

As highlighted earlier, developing India's digital economy is heavily dependent on how the PDP Bill is structured. In a way, having a robust and thorough law is a must to develop India's digital economy.

WAY FORWARD

Companies need to consider establishing transparent and accountable data protection matrices internally and while dealing with a third party, including emphasizing the role of grievance cells, focusing on building feedback loops into the design, providing accurate information on why processing is undertaken, measures deployed to mitigate breach and maintain data security, and start-ups should not be treated as an exception to this new norm. Quite naturally, we believe that start-ups will have to build in-house expertise and allocate resources in order to ensure that they create a trusted, transparent and accountable data processing and governance framework in accordance with what is spelt out in the law. From providing autonomy to the individuals to assert control over their personal data, to setting out standard data processing and governance practices for businesses, PDP 2019 will go a long way in establishing an equitable digital society.

In the absence of a data protection law and considering the data processing matrix is diversified between different organizations, an individual's ability to claim autonomy over their personal data is severely curtailed. A comprehensive data protection regime rightly must ensure that, but at the same time, there is a need to balance business and innovation interests, with a special focus on those fuelled by thriving start-up-startup and SMBs.

Start-ups and SMBs operate on funds that are usually earmarked for spurring innovation and aid in business growth. Increased compliance burden and regulatory uncertainty could add to the financial stress and might affect optimal use of limited resources at their disposal. Through the consultations over the course of 2020, we witnessed that start-ups are often left to choose between a false binary of privacy and security. This dichotomy is misplaced, and we believe that there is a need for increasing awareness, backed by sufficient boosting measures from the government that incentivizes and encourages the start-up ecosystem to view data protection principles and regulations as a value add, and a business enabler.

Ultimately, start-ups face a two-fold issue with PDP 2019 in its current form. Firstly, the compliance costs are high that may cause them to lose finances and prevent them from carrying their operations. Secondly, the uncertainty in the regulatory regime will discourage potential investors, and stifle innovation and risk taking. Thus, it is vital to have a clear timeline of implementation, and allow for an agile law that is dynamic to ensure that it is adaptable, and provides enough time for the start-ups to comply. As India moves from a state of no data protection, to a strong regime, there are bound to be some hiccups on the way. However, it is necessary to create progressive policies which minimise job loss and allow start-ups to thrive.

KEY RECOMMENDATIONS

KEY RECOMMENDATIONS

1. DEVELOP A COMPREHENSIVE TIMELINE FOR COMPLIANCE

Due to COVID-19, start-ups have been suffering from reduced revenues and have their operations impacted negatively. A recent survey revealed that 74% of start-ups and MSMEs expect to scale down or entirely shut down their operations over the next 6 months.[2] In addition, 78% of start-ups and MSMEs have reduced their workforce.[3] In such a scenario, the operational and structural changes under PDP 2019 will require start-ups to hire certain personnel, change management systems, processes of data collection, analysis and storage -- these compliances will impact certain start-ups more than others. Therefore, having a comprehensive timeline which is cognizant of the disruption caused by COVID-19 is vital.

2. PREPARE STAGGERED IMPLEMENTATION AND PROVIDE TIMELINE SPECIFIC EXEMPTIONS FOR BUILDING A GOVERNANCE AND COMPLIANCE CULTURE

Start-ups are going to be affected differently under the compliance standards of PDP 2019. Data driven start-ups and SMEs are at differing levels of funding, operations and management of their business models. The Dialogue's series of stakeholder consultations explored the challenges faced by start-ups which were set up relatively recently, and those who had been around in the market for some time. **Start-ups emphasized the need to have graded compliance standards, accounting for the differences in revenue and therefore, capacity.**

The ability to pay the penalties listed out in the PDP 2019 will differ - and for some start-ups, a steep penalty as envisaged in the PDP 2019 can economically impact their business models and cause them to falter. **Clause 57** of PDP 2019 lists out the penalties and compensations to be paid. It is unclear how these numbers are decided upon - for instance, the penalty for contravening certain clauses of PDP 2019 such as failure to register with DPA, obligation to undertake a data protection impact assessment by a significant data fiduciary (which could be a start-up that wishes to test new technology), and appointment of a data protection officer by a significant data fiduciary - can result in a fine of Rs. 5 crore/2% of its total worldwide turnover of the preceding financial year (whichever is greater).

3. CAPACITY BUILDING AND GUIDANCE RESOURCES

Start-ups require assistance and regulatory guidance to comply with the norms found in PDP 2019. Apart from the technical personnel they will have to hire, the regulatory experts will also require start-ups to invest capital for their services. For start-ups to achieve the goal of compliance and undergo a smooth transition from data protection under the Information Technology Act currently to the proposed PDP 2019, they would require various sessions and knowledge material towards capacity building. Despite these resources, regulatory compliance costs will still be significant - but it would provide a reasonable starting point for start-ups and SMEs to begin exploring options and evaluate their current standards of data protection with respect to PDP 2019.

[2] https://www.localcircles.com/a/press/page/covid-19-startup-sme-survey#.X5E-g9AzY2w
[3] https://www.nationalheraldindia.com/national/covid-19-78-msmes-and-startups-in-india-reduced-workforce-in-last-8-months-says-survey

4. FACILITATE INVESTMENT

Private equity financing in the form of venture capitalism (VC) could take a hit for start-ups in India, owing to the uncertainty caused by COVID-19. Add to that the regulatory uncertainty created by the lack of timelines due to the PDP 2019, and start-ups in India could witness the average time between making a pitch and receiving investment from VC funders. Data on VC funding during COVID-19 shows that the average deals in the months of 2020, as compared to corresponding months of 2019, have fallen significantly.[4]

Sectors such as fintech, ed-tech and health tech have picked up in India during COVID-19. The pandemic has led to a reliance of citizens on the digital economy, thereby resulting in the growth of these sectors. This also inevitably means that start-ups - even those that were not particularly data intensive - have shifted their business models to online modes. Therefore, more data than ever before is being collected, including categories of **'sensitive personal data'** as mentioned under **Clause 2, Chapter 1** of the PDP 2019. It is vital to keep investment flowing in these sectors - especially at a time when many start-ups, even those that are late-stage start-ups (which depend upon VC funding to expand their business models), are facing a crunch on funding and investments.

5. RESTRICT GOVERNMENT ACCESS TO START-UP DATA

Another major disincentive for start-ups to scale is the unfettered access given to Government agencies for lawful access to data held by these companies. It is pertinent to note that Clause 35 of the PDP Bill includes insights generated from data as well. At a time when resources are scarce, and the insights form a huge part of every start-up's business development- a framework that grants government agencies unfettered access might be a challenge to business interests. This also gives rise to fears surrounding surveillance. Proper riders on the powers of the state agencies, with clear processes for access must be laid out for ensuring fairness, equal treatment, and regulatory certainty. **Any access to information that is private, and where such access infringes on the right to privacy, must be qualified by the part test from the Puttaswamy judgement.**

6. ADDRESS IPR CHALLENGES

Stemming from the mandatory data sharing regime envisaged from the PDP framework, there are various views on what the future of IP rights would look like in a digital economy. There are popular analogies made about data, in its comparison to that of oil, to that of infrastructure of a digital economy and to that of oxygen. That being said, database owners have rights over them, subject to a few conditions, in the form of copyright. Some algorithms that are used for data analysis that yield insights are also protected under IP regime. Moreover, some argue that trade secret protection must be granted to key business intelligence to ensure competitive edge.

As it stands right now, there is no clarity on what the IP Framework will look like for data and allied data related assets, causing uncertainty and unease to the start-up communities. To effectively make use of the resources at hand, monetise and reap exclusive benefits from key insights,IP rights are crucial. Along with the conversations surrounding data governance, it is key to highlight the scope of IP laws to define the incentives available for various stakeholders in a digital economy and how it can be

[4] https://www.livemint.com/news/india/how-covid-19-has-changed-vc-investing-in-india-11592896613103.html

be leveraged for scaling.

It is pertinent to note that recommendations by the Committee of Experts on Non Personal Data Governance Framework recognises the IP protections associated with insights and databases. The report recognises the possible clashes with the existing IP regime, including India's TRIPS obligations that might be affected by such a regime.

7. ENSURE INTEROPERABLE LAWS

Interoperability has a positive impact on consumer choice, ease of use, access to content, and diversity, etc.[5] It helps in driving innovation, competition, accessibility, openness and flexibility. Countries globally are working to develop and implement data privacy frameworks that can adequately protect data of their citizens, while also allowing data to flow across borders in ways that support trade and innovation. These frameworks encourage convergence across the region, which enables data to flow while maintaining a similar level of protection. India must look at enacting similar frameworks based on the principles of adequacy and reciprocity with the EU, US, UK and other nations, to allow free flow of data across borders while protecting user privacy.

To support Indian start-ups' global ambitions, it is important to ensure interoperability in laws. This will allow the companies to operate in multiple jurisdictions, without additional overheads for compliance at every given stage. It is necessary to understand the Indian context, but at the same time, have multilateral engagements with like-minded countries for robust data governance. Many companies are already GDPR compliant, due to operating in European markets. For these companies, Indian law compliance would be slightly easier. However, for start-ups to start from scratch, and to comply with multiple laws at the same time, the impact on their resources would be drastic. An interoperable regime will unlock the benefits for a Indian startup to global markets, and is in line with the "Local for Global" campaign. The startups will be able to operate in the Indian market, for the global market with no additional overheads.

8. DEMARCATE THE SCOPE OF PDP AND PROPOSED NPD LEGISLATION

Clause 91 of the PDP bill empowers the state to gain access to insights and non-personal datasets that are held by companies and start-ups for advancing objectives of "public policy". The B2G data sharing in this regard might be better dealt with under a separate policy framework that aims to regulate the governance of NPD. Widespread powers, without going into the nuances and purposes for which data might be sought, paves way for arbitrariness. Clause 91 could stand as a possible violation of various proprietary insights that start-ups hold, confidentiality of information etc. In the absence of a regime that is clear on the procedure for access, this could be disruptive for many businesses that hold these insights and information to draw economic benefits from it. It is crucial that this clause is deleted from the scope of the PDP Bill, and it is recommended that the proposed NPD Governance regime is better suited to address this objective.

As mentioned earlier, the Committee of Experts has recognised that the two frameworks must exist separately, and the provisions regarding NPD will be covered entirely under a new legislation.

[5] Gasser, U. (2015). Interoperability in the Digital Ecosystem. Information Technology & Systems eJournal.

INTRODUCTION

SITUATING START-UPS AS A KEY STAKEHOLDER IN CONVERSATIONS SURROUNDING DATA GOVERNANCE

In a data-driven world, the start-up and SMB community stand to gain from the increased market opportunities available. The Government of India has identified the start-upup ecosystem as an integral part of building the nation - where there are **more job creators than job seekers**. India is the **third-largest start-up hub** in the world - and Startup India - the government's flagship initiative to incentivize the growth of start-upsups, technology, and innovation in India has estimated the creation of **187,004** direct jobs since its inception in 2016.[6]

The impact of COVID-19 on start-ups has led to reduced opportunities for funding innovation than before. This has led to an atmosphere of uncertainty and has inevitably led to the adoption of technology by start-ups that were hitherto not data/technology-driven. As more start-ups engage with technology, there are more use cases for artificial intelligence, blockchain, edge computing, internet of things, 5G, analytics, cloud computing and agile application developer tools. Quite naturally, start-ups and SMBs will be captured by the regulations pertaining to data governance, under PDP 2019 and the to be framed non-personal data regulation as suggested under the Report by the Committee of Experts..

As it stands right now, the engagement from start-up and SMB communities are minimal on matters pertaining to data governance policies. Through a series of stakeholder consultations, we received first-hand inputs from data intensive start-ups on the pressure points with the proposed policies.

IMPACT OF THE PDP BILL ON START-UP AND SMB ECOSYSTEM: AN OVERVIEW

The Indian start-up ecosystem could confront certain challenging times and the most striking instance is the delicate balance that they have to instill for respecting the rights-based regime contemplated under sector agnostic, omnibus, privacy centric PDP 2019, with their requirements of digital economy and data focused innovations. The objects clause of PDP 2019 clearly acknowledges the need to scale and innovate. Prima facie, they balance as contrasting themes, as implementing rights regime will require compliances, and innovation requires some flexibility. To balance conflicting scenarios, it states that a key objective of PDP 2019 is to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensures empowerment, progress and innovation through digital governance.

It is natural that PDP 2019 will impose compliance costs on firms that will demand utilization of existing resources, which will require entities to reallocate their resources from other operations - involving operational scaling.his could mean lesser allocations for investing in innovations. Research shows that regulations are per se counterproductive for innovation and competition in the short run. [7]

[6] https://www.business-standard.com/article/economy-policy/startup-india-initiative-created-over-560-000-jobs-since-2016-says-govt-119060401491_1.html

[7] Blind, K. (2012). The influence of regulations on innovation: A quantitative assessment for OECD countries. Research Policy, 41(2), 391– 400

However, regulations that aim at creating a governance structure (case in point corporate governance matrix under Companies Act and similar laws across the globe, employment laws and so on) are an important tool to create brand value, gain traction, foster consumer trust, and thereby positively impact demand for the goods and services offered by regulated companies.

In the current times, where individual lives intersperse with technology at every moment, this rationale becomes even more prominent for creating and sustaining demand for new technologies. However, there is truth to the proposition that SMBs can consider regulation as an overhead and operational/expansion hurdle.[8] If the regulations are onerous, it makes it harder for the companies to innovate a product that is compliant with regulations and also holds market value. This is a conundrum that many Indian start-ups are dabbling today with the introduction of PDP 2019. In this scenario, it is important to remember the shift in regulatory position for listing of start-ups. From a time where start-ups were disincentivized to list on India stock exchanges because of the rigorous listing thresholds, to now, when separate start-up platforms are hosted by stock exchanges and more and more start-ups are likely to soon come with their IPOs, it is not misplaced to urge for simpler compliance and to address this conventional debate between regulations that have to be tailored in a way that incentivizes startups and emerging businesses.[9] In January 2020, Tranway Technologies performed well in its IPO - by getting oversubscribed 1.88 times than the company had projected.[10]

At a time when PayTM Money is allowing users to participate in its upcoming IPO, there is a positive atmosphere around investment in the startup ecosystem in India. Companies are expected to target a broader base of investors, and the idea for startups is to create a more accessible process for those willing to invest.[11]

Through governance versus innovation, Clause 40 of PDP 2019 provides for a regulatory sandbox mechanism, and the efficiency of the contemplated provisions is analysed subsequently.

To explain, let us consider the case of consent as provided under PDP 2019. Clauses 7 (notice for collection and processing of personal data) and Clause 11 (consent) provide for a rigorous standard and threshold for informed consent. The objective is to make consent exercise meaningful, where the data principal is fully cognizant of what, how, where and when data is being processed. But, a corollary to this is that consent requirements will severely limit the extent to which start-ups can reprocess the data for driving innovation, at every point in time it is processed for innovation, research and development. However, whether such a generic statement will satisfy the specificity expected under PDP 2019 cannot be tested at this stage, and consequently, a literal interpretation will suggest that in the data lifecycle, specific, express and clear consent must be obtained, purposes as required by principle of purpose limitation sought to be implemented through a intertwined mechanism of notice, consent and access rights of principals. This is likely to cause 'consent fatigue', where multiple legitimate interests or repurposing notices are provided to the data principal.

Another instance where PDP 2019 could stifle innovation is regarding its clauses around data localisation. Chapter VII mandates that sensitive and critical personal data is stored within India. It also requires that critical personal data be only processed

[8] Stewart, L. A. (2010). The impact of regulation on innovation in the United States: A cross-industry literature review.
[9] https://www.financialexpress.com/industry/sme/bse-startups-platform-gets-its-fourth-ipo-tranway-technologies-issue-subscribed-nearly-twice/1840573/
[10] https://economictimes.indiatimes.com/markets/ipos/fpos/tranway-technologies-zooms-17-on-market-debut/articleshow/73965240.cms
[11] https://www.livemint.com/market/ipo/paytm-money-to-offer-investments-in-ipos-11606670138804.html

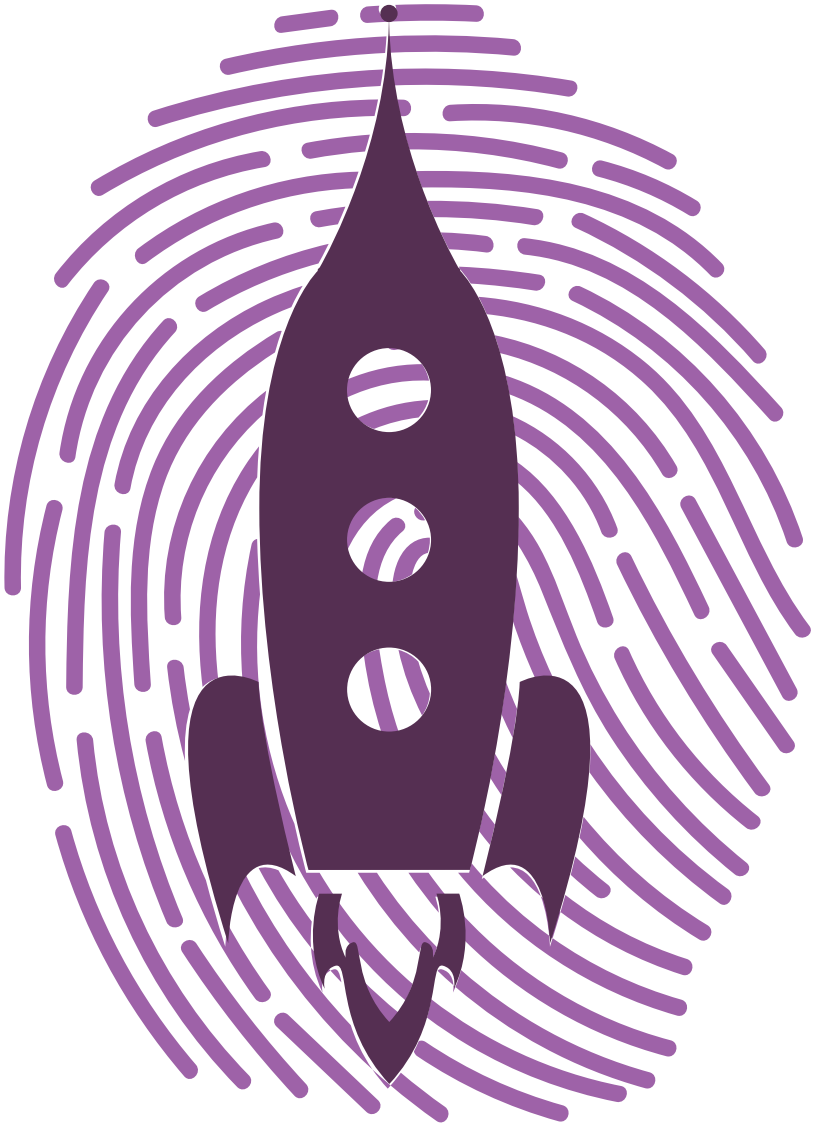
in India. This will increase compliance cost and at the same time pose restrictions on free flow of data in a global setting, adding to the toll that start-ups have to bear in order to stay in the market, making their production costs higher, which could force them to shift some of this burden to their end customers. Cutting of data flows or making them more expensive through a regime of ambiguous regulations will hinder local or domestic companies from global participation, and suppress their ability to participate in the global digital economy in the long run.[12] Furthermore, it has been observed that data localisation laws have consequences to follow for companies that work in these jurisdictions. When data localisation is mandated, it deters foreign companies from interacting with such companies as their compliance structure is non-consonant with the international data business models currently in play across the globe.

PDP 2019 also sets out that anonymized, non-personal data can be sought out from any data bank as the government pleases. This is a cause for serious concern, as many start-ups rely on the integrity of their data sets and the insights they glean out of it as their primary business model. Not offering any compensation, or not providing clarity about the purposes for which these data sets are used, or guidance on how intellectual property arising out of such data will be protected, could lead to arbitrary yielding of power by the government.

A regulatory sandbox envisaged in the bill (Clause 40) is particularly useful as far as the start-ups are concerned. This enabling provision will allow start-ups to innovate and avail exemptions from PDP requirements, while dealing with innovative technology pertaining to AI, machine learning or other emerging technology for public interest. However, the DPA has to first vet if the company meets the privacy-by-design requirements that are set out. In a way, it is imperative that as part of the sandbox, the innovative technology is thoroughly evaluated through proper data protection impact assessment, and perhaps, the cost for such analysis should be provided as an incentive under the sandbox mechanism. This is a welcome move and is likely to encourage start-ups to innovate on matters of public interest. That being said, there is a need to assess if the DPA has the regulatory capacity while deciding on these crucial, yet technical questions.

[12] IAMAI (2016); UNCTAD (2016)

ANALYSIS OF PROVISIONS OF THE PERSONAL DATA PROTECTION BILL 2019



ANALYSIS OF PROVISIONS OF THE PERSONAL DATA PROTECTION BILL 2019

1. CLEARER DEFINITIONS AND REGULATORY UNCERTAINITY

The primary concern is centered around the need for clearer definitions of what constitutes 'sensitive personal data' and how to classify it. As it stands right now, almost every piece of personal data can be covered as sensitive personal data. This is based on a literal interpretation of the definition, which reads (clause 3(36)) –

> "SUCH PERSONAL DATA, WHICH MAY, REVEAL, BE RELATED TO, OR CONSTITUTE (I) FINANCIAL DATA, (II) HEALTH DATA, (III) OFFICIAL IDENTIFIER, (IV) SEX LIFE, (V) SEXUAL ORIENTATION, (VI) BIOMETRIC DATA, (VII) GENETIC DATA, (VIII) TRANSGENDER STATUS, (IX) INTERSEX STATUS, (X) CASTE OR TRIBE, (XI) RELIGIOUS OR POLITICAL BELIEF, (XII) ANY OTHER DATA CATEGORISED AS SENSITIVE PERSONAL DATA UNDER SECTION 15."

Inclusion of words like "related to" and "constitutes" is wide enough to include every personal data. For instance, surname reveals caste in India, and hence, surname will be sensitive data. Similarly, age reveals risk for contracting COVID-19 and hence, yet again a potential sensitive data. Further, PDP 2019 states that additional categories of "sensitive personal data" can be notified by the DPA as and when required, and "critical personal data" is not notified.

This may cause apprehension to both start-up owners and investors, and brings about regulatory uncertainty to start-ups with regard to the data practices to follow for each set of data. Further, it is important to highlight that the obligations and compliances attached to different kinds of personal data are separate, which would mean that planning is crucial in the operational and data management strategies. Case in point – data localisation (clause 33), conducting data protection impact assessments on deploying new technology for sensitive personal data (clause 27), additional consent requirements (clause 16), and so on. Uncertainty in the scope and overall regulatory framework is contrary to well-designed data governance models. It dilutes planning and strategy, misaligns the actual steps that are required, and ultimately, will result in erroneous allocation of resources to meet compliance requirements. This should be avoided to make the scope clearer and to remove ambiguity around definitions of sensitive personal and critical data.

2. ACCESS - GOVERNMENT AND PRIVATE

PDP 2019 as it currently stands, under clause 91, allows for access and use of anonymised and non-personal data for framing any policy for the digital economy, measures for its growth, security, integrity, and prevention of misuse. The government may, in consultation with DPA, direct any data fiduciary or data processor to provide any anonymized or non-personal data to enable better targeting

of delivery of services or formulation of evidence based policies. In this context, non-personal data has been referred to as any data other than personal data, and as such this can include proprietary and confidential data such as trade secrets, market strategies, consumer insights, know-how, etc. While it may seem premature, the proposed clause allows the government to come up with directions, and there is no clarity on what, why and when such directions will be issued. Across The Dialogue's consultation and through different groups of participants, there emerged a trend of start-ups pointing out that this unfettered access could deter innovation, and discourage investors from coming into India. They also pointed out the IPR conflicts, as government demands for business intelligence could affect the competitive edge these companies hold.

Most of the participants across The Dialogue's consultation group stated that the universe of non-personal data, including anonymised data sets, are vast. For example, non-personal data includes data sets aggregated and collected by various mobile applications and websites on the internet, arising from the digital trail that individuals leave in the wake of their website usage. It also includes anonymized data sets arising from the behavioral patterns of users on social media intermediaries. Furthermore, the consultations revealed the challenges regarding the notion of individuality.

In contrast with personal data, which can be traced back to an individual, the critical difference between personal and non-personal data arises from the fact that it challenges the notion of individual control over data as individuals are unlikely to be aware of what their personal data can reveal when aggregated with a multiverse of other data points. Further, there have been concerns on why should the DPA, who is primarily responsible for regulating the personal data regime, be allowed to advise the government on matters concerning non-personal data. Since the purpose of PDP 2019 is to protect the personal data and privacy of individuals, clauses relating to state access must align with the objectives and must be limited to that extent. Clause 2 of PDP 2019 categorically states that anonymized data is outside the purview of PDP 2019, and at the same time, clause 91 creates a completely opposite stance, where the government will rely on clause 91 to actually deal with anonymized data. It may therefore be prudent to revisit clause 91, and delete it from PDP 2019.

3. FREE FLOW OF DATA AND INTEROPERABILITY WITH GLOBAL REGULATORY LANDSCAPE

Interoperability in data protection laws across the world exists to keep the spirit of competition between companies alive, without compromising on privacy. Without interoperability of technology tools as well standardization of processes, new companies would not be able to train their machine learning and AI models, due to barriers of access to existing datasets. Interoperability, in both these manifestations, helps to enhance the effectiveness of data by presenting or storing in standardized models, coupled with easy data transfer protocols to enable knowledge and insight sharing. For instance, the National Draft Health Policy stresses on the need for interoperability of datasets in the healthcare ecosystem for the objective of providing universal health care access.

Though achieving it may incur costs to institutions and entities, its long-term payoffs ensure that the trade-off between cost and benefit is fair. In the context of data protection, interoperability is a precondition for the interconnectedness and free flow of data that is crucial for a data-based economy, and therefore for data-driven innovation.[13]

[13] Wolfgang Kerber and Heike Schweitzer, Interoperability in the Digital Economy, 8 (2017) JIPITEC 39 para 1. https://www.jipitec.eu/issues/jipitec-8-1-2017/4531/JIPITEC_8_1_2017_Kerber_Schweitzer.pdf

Across The Dialogue's consultation groups, participants on multiple occasions, while explaining multiplicity of compliance issues, aired their grievance with the 'non-harmonized' nature of PDP 2019 when it comes to globally accepted and enforced privacy standards. The participants called for consonance between international and domestic definitions for greater ease in evolving international standards for data governance. For instance, European Union GDPR allows companies to process personal data for repurposing as well. Repurposing is any new purpose that originally was not consented to. The condition to be satisfied in such cases is to ensure that the repurposing of data is not prejudicial or does not harm the concerned individual in any manner.

Similarly, EU GDPR provides for a much more matured and progressive scope of the right to be forgotten. Considering a scenario where PDP 2019 does not establish standards for protection that are compatible with other international frameworks, India might not match up to adequacy standards for the purpose of cross border data sharing. The recent example of the EU-US privacy shield, that was struck down by the Court of Justice of the European Union signals towards the need for developing internationally compatible standards. This could be achieved by establishing greater synergy between sectoral regulators as data transfer surpasses any one industry regulator's jurisdiction. It is therefore, in everyone's best interest that intersectoral synergy is developed while regulating transfer of personal data.

While discussing the contours of this synergy, the panelists in our consultations opined that the nature of this synergy to be one that is both judicial and industry specific in nature. The judicial oversight mechanism, within the processes of the regulators, will ensure transparency and impartiality. Since various sectoral regulators that already exist operate differently, the industry practices that are in place must be taken into consideration when cooperation is established. The modalities of synergy between the regulators can be laid out with mutually agreeable MoUs, to demarcate roles and responsibilities. This could also include routine data sharing/information sharing, cooperation for other administrative matters, etc. They also opined that a failure to achieve this would result in a broken system that would not be able to enforce agreed upon standards, thereby, nullifying any progress of regulation in the first place.

Takeaway: PDP 2019 should enable free flow and interoperability of data. Moreover, the Bill should try to harmonise concepts and regulations with international standards of data governance.

4. STRUCTURE OF THE PROPOSED DATA PROTECTION AUTHORITY (DPA)

Enhancing independence of the data regulator is essential for ensuring privacy. The discussants opined that there is a need to enhance the technical expertise in the composition of DPA. Clause 42 regarding the same reads vaguely and there is no distinction made between technical members and regular members as seen in other regulatory bodies such as the Telecom Regulatory Authority of India (TRAI). It was pointed out for assessing privacy risks and to effectively grant permissions for innovation sandbox and for ensuring privacy by design requirements, technical capacity would be vital.

The DPA has been empowered to issue codes of practice with respect to various matters such as conditions for valid consent, methods of de-identification and

anonymisation of data. These codes of practice, if violated, can be considered to be a violation of PDP 2019. It will prove difficult for all data fiduciaries and data processors to comply with a uniform code of practice, as it may put small businesses such as start-ups at a disadvantage. To solve this issue, it might be prudent for the DPA to create a separate code of practice for the ecosystem.

The DPA must be a dynamic regulator, that looks at regulation of a universe as vast as data as a collaborative process. It must aim to harmonize the functions of existing regulators and facilitate inter regulator synergy. As an overarching regulator tasked with the aim of protecting the integrity of the data principal's personal data, DPA must work closely with the sectoral regulators to evolve better data practices and be a thought leader in data governance across the world.

Takeaway: Clauses concerning DPA's composition and functions must be relooked at in the PDP 2019. There must be consonance with other regulators such as the TRAI and CCI.

5. PROPOSED CONSENT MODELS

Multiple participants across The Dialogue's consultations identified the issues surrounding consent as a pain point. Consent fatigue would weaken the true intent of the provisions, as standard forms of deriving consent are heavy on legalese. It is important that consent must be sought in accessible form, and is clear. A start-up founder pointed out an example regarding collection of consent and the importance of context of collection. When it comes to health data, and consent is sought in this context, it would automatically be in the favour of the doctor/authorities, since the patients prioritise the treatment. Many beneficiaries of the Ayushman Bharat Scheme, the state sponsored health coverage program, fall within the lower income bracket, and they follow this trend, the participant claimed. This would make compliance hard, unless clear standards for consent is specified, that can be adhered to during collection and processing of data.

The consent manager mechanism was brought out during the course of the discussion. The account aggregator model adopted in the financial sector was cited, along with the national health stack that was currently in development. There was widespread agreement that there needs to be clearer provisions that address issues of consent in PDP 2019. A panelist raised a question regarding withdrawal of consent provision in the Bill. If a business builds on a product/design analytics, after taking valid consent from a data principal, withdrawal of consent at a later state might be a detriment for long term plans.

Takeaway: PDP 2019 should allow alternatives to consent as the basis of processing, such as legitimate business interest and repurposing as long as data principal's rights and interests are not harmed.

6. POTENTIAL IMPACT ON INVESTMENT

PDP 2019 does not, at present, ensure smooth consonance between domestic and international law (such as the GDPR) pertaining to treatment of personal data. Without this issue being addressed, and without a mediated process to implement data protection policies which do not disturb investor sentiments, Indian start-ups might face greater operational challenges.

In relation to foreign investment and global investment sentiment over the proposed added compliance regime mandated by PDP 2019, there needs to be a critical enquiry into the possibility of investor sentiment becoming negative and bound to evolve with the increased public oversight over their data. India's credibility comes from being an 'investment friendly nation', and our past record as being a country which is attractive for foreign investment drives the Indian dream of a Trillion dollar digital economy. With steep compliance burden and regulatory uncertainty, this is likely to get affected and could prove to be disruptive. The main issue isn't necessarily the compliance requirements itself, but rather the clarity of how the same is going to be implemented; on whom and to what degree, which could potentially impact investments in the future.

Takeaway: Provide greater regulatory certainty in the domestic legislation and evolve it with interoperability at the core of such regulation. This will aid in driving innovation and investment from global players, in the Indian startup ecosystem.

FURTHER CONSIDERATIONS

FURTHER CONSIDERATIONS

1. BUSINESS CONSIDERATIONS

THERE ARE SEVERAL CONSIDERATIONS FOR THE BUSINESS MODELS OF START-UPS WHICH HAVE BEEN OVERLOOKED IN THE DRAFTING OF THE PDP 2019. GOVERNMENT ACCESS TO PERSONAL DATA COLLECTED BY ORGANISATIONS, A LACK OF INDEPENDENT THIRD-PARTY REPRESENTATION IN DECISION MAKING, AND THE LACK OF A CLEAR PROTOCOL FOR SHARING DATA WITH THE GOVERNMENT ARE ALL POTENTIALLY CHALLENGING AREAS FOR START-UPS.

PDP 2019 accords unfettered access to personal data to the State under clause 35. The clause "seeks to empower the Central Government to exempt any agency of the Government from application of the Act."[14]

Here, it is critical to understand that any access must be backed with reasonable checks and balances, as enshrined in the Puttaswamy judgment. Several landmark decisions of the court clearly have expounded that any fundamental right can only be suspended, provided due process of law is followed. Due process requires substantive as well as procedural norms. These are left out of the ambit of clause 35, and a recorded order can be passed for the government to suspend the data protection measures under PDP 2019. The Bill at Clause 12 provides for certain grounds of processing, where consent is not required, and this already enables the government to derogate from the fundamental principle of processing (i.e., processing must have a lawful basis) in discharge of its functions or under any law for the time being in force. As such there is no need to exempt any government agency for disregarding all other provisions of PDP 2019, should the government deem that such need or exigency exists. This strikes at the basic rule of proportionality. For start-ups, this unfettered access can hamper their business models in various ways. For example, in cases where data and associated insights provides competitive edge to the business, unfettered access without clear procedure could give rise to abuse of such power.

Another aspect that PDP 2019 lacks is third party representation in decision making. For instance, the structure of DPA does not seem to coordinate with private players such as start-ups, and it seems to exist primarily for penalizing them. Such composition can be used to consolidate decision making power into the hands of the Government in power, and with changes in political scenario, the DPA views can be varied.

For the start-up community, there is a need for a clear protocol for data sharing with the government under PDP 2019. At present, because the procedures are ambiguous, this creates challenges for how, when and what data the government can have access to and how it shall be used. This is natural as many start-ups leverage their data sets to derive proprietary, price-sensitive information that is protected by confidentiality and can qualify as intellectual property in the prevalent sense of the term. Sharing such data could be challenging for their business outcomes and once procedures are established, it will help put businesses at ease.

[14] http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

2. COMPLIANCE COST

> **It is impossible for Indian start-ups - especially early-stage start-ups - to be compliant with multiple domestic and international laws at the same time. To reduce compliance burden on start-ups, PDP 2019 should mark out categories of start-ups given their present business models, funding and stage of growth - to help start-ups operate on a limited budget.**

The 'Make in India' initiative is a good policy decision and a benchmark to be re-imagined in the data sector if policy makers wish to ensure survival of domestic data driven companies. It is important to focus on capacity building and hand holding of smaller companies in regards to compliance is necessary to ensure their survival and will go a long way in actualizing the Prime Minister's new *'Atmanirbhar'* ambition of India.

To ease the troubles of the start-up and SMB communities, there must be a carve out that would have different, and relaxed standards of compliance. This could be based on a financial threshold, and could help these companies plan out compliance, and make their business better. It is important to ensure that there is a relook on the liability regimes under the Bill, as non-compliance will lead to drastic measures from DPA. This would stifle innovation, as many would be fearful of criminal prosecution. There needs to be a relook at how we envision liability regimes for data governance. There needs to be a graded model of liability, and a one-fits-all strategy will not be helpful. The need for this model is particularly important given that the start-ups and SMBs operate with limited resources.

CONCLUSION

The stakeholder consultations organised by The Dialogue with members of the start-up and SMB communities in India made it clear that there is a need for nuanced conversation around a progressive data regime. Start-ups face regulatory uncertainty due to the Personal Data Protection Bill 2019 on multiple counts - on the one hand, regulation imposes compliance costs on firms, sapping resources otherwise available for productive activities, such as innovation, or raising entry barriers, thus reducing competition and incentives for innovation.[15] However, regulations can also foster consumer trust, thereby increasing the demand of new technologies. When faced with a situation where the firm that comes up with an innovation struggles with a regulatory hurdle, compliance innovation aids the firms to push ahead, without being on the wrong side of the law.[16] If the regulations are onerous, it makes it harder for the companies to innovate a product that is compliant with regulations and also holds market value. This is a conundrum that many Indian start-ups face today with the introduction of PDP Bill 2019.

India needs a strong data protection regime which factors in the globalized nature of start-ups. For instance, there are data services for storage which are located in other countries, which are used by start-ups in India as an integral part of their business model. The Personal Data Protection Bill 2019 drastically penalises start-ups and does not offer enough clarification or time for compliance. It is an urgent need for public policy discourse around technology policy to flag this as a massive hurdle for Indian start-ups, especially during uncertain COVID-19 times. Any pressure on the start-up and SMB community at the moment could spiral into job loss and reduced economic growth. Therefore, the Personal Data Protection Bill 2019 needs to be reflective of these concerns and come up with solutions for the same.

It is necessary for India to look at international definitions whilst building new definitions for India. This would help global regulators be in tandem with India's new DPA.. Multiple regulators need to proactively be encouraged to work together so that they can encourage and enhance the functioning of start-ups and SMBs. Another need of the sector that should be focussed upon is building technical capacity for both the judiciary and the regulator to be able to deal with the business related issues that arise around protection of personal data.

State capacity plays a vital role in ensuring a smooth transition, and the proposed DPA must look into ensuring minimal disruption. The start-up community feels the need for sector specific focus to allow nuance in the legislation, and to not adopt a one rule-fits-all solution approach in the bill. Government access to data collected, and processed by companies for the purpose of public policy decisions was part of the discussions, and many opined that the Bill should have a defined scope within which such data sharing can occur.

[15] Blind, K. (2012). The influence of regulations on innovation: A quantitative assessment for OECD countries. Research Policy, 41(2), 391– 400
[16] Stewart, L. A. (2010). The impact of regulation on innovation in the United States: A cross-industry literature review.

About the authors

Arya Tripathy is Partner at PSA (Priti Suri and Associates)

Karthik Venkatesh is the Research Coordinator at The Dialogue. His interests lie in the intersection of Data Governance and regulation of emerging tech. At the Dialogue, he heads the research efforts on Non Personal Data Regulations and leveraging data for effecting societal change.

Trisha Pande is the Policy Manager at The Dialogue. She is interested in the intersec-tion between technology and development studies. At The Dialogue, she works on a range of policy issues to make the internet a safer space for all. She currently leads research on gender and technology.

Imprint

Arya T., Karthik V.V., Trisha P., (January 2021). IMPACT STUDY: PERSONAL DATA PROTECTION BILL ON THE START-UP ECOSYSTEM. New Delhi. The Dialogue.

The Dialogue is a public-policy think-tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues.

This publication is part of The Dialogue's larger initiative to drive informed discussion on Data governance and Privacy, through a series of consultations and research.

www.thedialogue.co

The Dialogue™
INFORM ENGAGE IDEATE