Initial Comments of Dvara Research dated 16 January 2020 on the Personal Data Protection Bill 2019 introduced in the Lok Sabha on 11 December 2019

Dvara Research[1] is an independent Indian not-for-profit research institution guided by our mission of ensuring that every individual and every enterprise has complete access to financial services. Our work seeks to address challenges for policy and regulation in India given the waves of digital innovation sweeping financial services, focussing on the impact on lower income individuals in the country. The regulation and protection of consumer data has been a core area of our recent research.

In this document, we present our initial comments on the Personal Data Protection Bill 2019 (the Bill), introduced in the Lok Sabha in December 2019. This continues our engagement with the public consultation process on India's new data protection regime since 2017.[2] We welcome the introduction of the Bill in Parliament as an important development to take forward India's journey towards an overarching data protection framework. However, we are deeply concerned that aspects of the latest draft of the Bill could endanger users' data protection and hamper the growth of a free and fair digital economy. Seven key concerns are presented in this document.

1. User protections must be strengthened for the Bill to genuinely guarantee data privacy for Indians.
2. The Data Protection Authority has been weakened in the Bill, limiting the effectiveness of the new regime.
3. Immense powers and exemptions for the State will severely limit the effectiveness of the new regime.
4. The Bill should strengthen consumer protections within the proposed sandbox and clarify its objectives.
5. "Harm" should not be a condition on which rights and obligations depend in the Bill.
6. The Bill should not include provisions relating to the sharing of Non-Personal Data.
7. The Bill should contain transitional provisions to create certainty about its implementation.

We welcome your feedback and challenge on these initial comments to refine our thinking as the legislative process unfolds.

[1] Dvara Research has made several contributions to the Indian financial system and participated in engagements with many key regulators and the Government of India. Through our recent work we have extended research inputs to various bodies, including the Committee of Experts on Data Protection under the Chairmanship of Justice B.N. Srikrishna, the Ministry of Electronics & Information Technology (MEITy), RBI's Expert Committee on Micro, Small & Medium Enterprises and the RBI's Committee on Deepening of Digital Payments.

[2] Our primary research on Indians' privacy attitudes was cited in the White Paper of the under the Chairmanship of Justice B.N. Srikrishna of 27 November 2017. Our regulatory proposals on enforcement and the design of the Data Protection Authority (DPA) were specifically acknowledged and relied upon in the Final Report of the Committee dated 27 July 2018.

Summary of Comments

1. **User protections must be strengthened for the Bill to genuinely guarantee data privacy for Indians.**
    1.1. The Bill should not remove obligations to give notice to individuals where their personal data is processed without consent.
    1.2. The Bill continues to disincentivise and penalise withdrawal of consent, constraining individuals' "free" consent.
    1.3. The Bill must widen the suite of users' rights to meaningfully empower them.
    1.4. Exercise of rights should be allowed at no/nominal charge, to avoid excluding poorer Indians.
    1.5. The Bill should not restrict users' right to seek remedies.
    1.6. The Bill must mandate the notification of all personal data breaches to the DPA.
    1.7. The Bill should strengthen obligations for data fiduciaries to incorporate Privacy by Design.
2. **The Data Protection Authority has been weakened in the Bill, limiting the effectiveness of the new regime.**
    2.1. Changes to the design and composition of the DPA diminishes its independence as a regulator.
    2.2. Substantive powers and functions of the DPA that have been removed should be re-allocated.
3. **Immense powers and exemptions for the State will severely limit the effectiveness of the new regime.**
    3.1. The wide powers delegated through section 35 without clear guidance and safeguards on its use opens it up to constitutional challenge.
4. **The Bill should strengthen consumer protections within the proposed sandbox and clarify its objectives.**
    4.1. Consumer protection safeguards are completely absent in section 40.
    4.2. The objectives of the sandbox are unclear which could result in overlaps with other sandbox efforts (such as the RBI Sandbox).
5. **"Harm" should not be a condition on which rights and obligations depend in the Bill.**
6. **The Bill should not include provisions relating to the sharing of Non-Personal Data.**
    6.1. Provisions unrelated to the objectives of personal data protection should not be included in the Bill.
    6.3. Other complications arise if provisions relating to non-personal data are included in the Bill.
7. **The Bill should contain transitional provisions to create certainty about its implementation.**

References

1. User protections must be strengthened for the Bill to genuinely guarantee data privacy for Indians.

We set out seven aspects of user protection that are weakened in the latest draft of the Bill below. These relate broadly to the weakening of obligations to provide notice and take consent, constraining of rights of data principals, and limitations on protections afforded by breach notifications and Privacy by Design obligations.

1.1. The Bill should not remove obligations to give notice to individuals where their personal data is processed without consent.

The Bill provides certain grounds for non-consensual processing of data in section 12 (*grounds for processing of personal data without consent*). Nonetheless, even where these non-consensual grounds are used to process personal data, notice is required to be given to users to inform them of this under section 7(1)(e) (*Requirement of notice for collection or processing of personal data)* of the Bill. Such notices help to keep users informed of the use of their personal information. Unfortunately, a wide exception to the rule that notice must be given (even for non-consensual processing) has been introduced in section 7(3) of the Bill which enables entities to dispense with providing notice for any non-consensual processing of personal data. This provision should be limited only to cases of severe emergency (as was the case in the previous version of the Bill).

As per section 7(3) (*Requirement of notice for collection or processing of personal data)* of the Bill, providers need not give notice to individuals where it could "*substantially prejudices"* the processing of personal data on *any* of non-consensual grounds. In contrast, the previous version of the Bill (in section 8(3)) only allowed for notices to be dispensed with in cases of medical emergencies, responding to disasters, epidemics or breakdown of public order. This change in the new Bill problematic because it increases opacity in the operations of data fiduciaries in their non-consensual data processing activities, creating a complete information asymmetry between the data fiduciary and the data principal. This will directly and adversely affect users' ability to assess how their data is being used and identifying contraventions in the processing of their data. It severely limits the information that data principals have on the use of their personal data, and potentially disenfranchises them from exercising their rights under the Bill.

Accordingly, the requirement to give notice to users whenever their data is processed without their consent should be retained in the Bill. Limitations to this requirement should only be allowed in cases of severe emergency (as was the case in the previous version of the Bill).

1.2. The Bill continues to disincentivise and penalise withdrawal of consent, constraining individuals' "free" consent.

Section 11(6) (*Consent necessary for processing of personal data)* of the Bill makes the data principal liable for all legal consequences for the withdrawal of their consent for processing personal data, if the

data principal does not have a "valid reason" for withdrawal. There should be no barriers to withdrawal of consent for a data principal. This is already recognised in section 11(1)(e), which states that consent should be capable of being withdrawn with "*the ease of such withdrawal comparable to the ease with which consent may be given*". The threat of legal consequences would be a major disincentive for any data principal seeking to withdraw their consent for data processing. It could put the data principal in a situation where their personal data is retained under duress, calling into question whether their consent can be considered "free" (Rao, 2003).

Accordingly, we propose that withdrawal of consent should merely result in a simple termination of contract and related services to the data principal. Section 11(6) should not include language that places liability for all legal consequences of withdrawal on the data principal.

1.3. The Bill must widen the suite of users' rights to meaningfully empower them.

The Bill contains a very limited set of four rights for data principals. These are (i) right to confirmation and access (ii) right to correction and erasure (iii) right to data portability and (iv) a right to be "forgotten" i.e. preventing disclosure of personal information in certain circumstances. The absence of a full suite of user rights could result in the scales being tipped against users who may seek to achieve more autonomy and control over their data. The Bill must be expanded to include the following rights (as further detailed in (Dvara Research, 2018a)):

- right to clear, plain and understandable notice for data collection;
- right to be asked for consent prior to data collection;
- right to adequate data security;
- rights to privacy by design (including privacy by default);
- right to breach notification;
- right relating to automated decision-making;
- right to informational privacy;
- right against harm.

Some of these rights exist as obligations for data fiduciaries in the Bill (e.g. the need for a Privacy by design policy in section 22, Security safeguards in section 24, or reporting of personal data breach in section 25). They must also be included as rights of the data principals, to empower individuals to take recourse against data fiduciaries where they fail to provide these protections. This will strengthen individuals' position as they become aware if their information is being collected or used inappropriately. If this Bill truly seeks to empower and protect users in India, it must take into account the imbalance of power between the data fiduciary and data principals when it comes to the use of personal data in the digital economy. Our primary research on Indian data principals' experiences with the digital economy reveals that they have very few tools and little agency to exert their autonomy and

protect themselves from harms and misuse of their personal data (CGAP, Dalberg & Dvara Research, 2017). An important way to set right the imbalance between entities that process data and data principals is to enshrine the full bouquet of rights required in a user-friendly legal paradigm in the law. The Bill must be expanded to include a fuller set of rights for data principals.

1.4. Exercise of rights should be allowed at no/nominal charge, to avoid excluding poorer Indians.

Section 21(2) (*General conditions for the exercise of rights in this Chapter)* of the Bill erects a barrier for the exercise of certain rights of data principals by allowing for the charging of "*such fee as may be specified by regulations*". The proviso to the section limits the ability to charge fees for exercise of certain aspects of certain rights. It is submitted that exercise of the remaining rights should also be at no or at a nominal fee (if the intention of the fee is to create friction for spurious requests to exercise rights).

Income levels in India remain low. In 2018, the Gross Domestic Product (GDP) per capita in India was US$ 7,762. This is considerably lower even compared with the figures for countries with similar level of development like Brazil (US$ 16,096), Mexico (US$ 19,844) and South Africa (US$ 13,686) (The World Bank, 2018). However, this has not held millions of Indians back from using and navigating digital interfaces. As awareness of data sharing and related rights grow in our society, people across different strata of society will seek to exercise their rights under this Bill. Given the Indian context, a fee would be serious barrier to exercise of rights. This is troubling for the users themselves, as well as the system as a whole given that the data principals who exercise these rights play an important role of adding to the data quality of the entire system.

Accordingly, it is submitted that exercise of rights should be at no fee or a nominal fee only.

1.5. The Bill should not restrict users' right to seek remedies.

Section 83(2) (*Offences to be cognizable and non-bailable)* of the Bill states that a court can take cognisance of an offence only when a complaint is filed by the DPA. This provision prevents the data principal from directly filing the complaint to the court when an offence is committed under the proposed Bill. Instead the individual whose right is violated needs to make a complaint to the DPA, and only the DPA can file the complaint to the court.

Similarly, the proviso in section 63(1) *(Procedure for adjudication by Adjudicating Officer)* restricts individuals from initiating civil inquiries under the data protection regime, by providing *"that no inquiry under this section shall be initiated except by a complaint made by the Authority*." This implies that individuals must approach the DPA to register any civil complaints. Taken together with the fact that there is no other provision in the Bill that empowers the individuals to appeal against the DPA, the

individual has no right to a remedy if the DPA does not file a complaint or initiate an inquiry pursuant to her complaint.

Both these provisions violate the right to seek remedy of the individual, which has been confirmed by the Supreme Court when it struck down a provision identical to section 83(1) in the Aadhaar Act. The Aadhaar Act had an identical provision under section 47 which barred the court from taking cognisance of the offence unless the complaint is filed by the Authority (UIDAI). The Supreme Court held that this provision was arbitrary as it fails to provide a mechanism to individuals to seek efficacious remedies for violation of their rights (Justice K.S. Puttaswamy (Retd) & Anr v. Union of India & Ors, 2018) . It is highly likely that in their current form section 83(2) and the proviso to section 63(1) will fall foul of the test of arbitrariness as set out by the Supreme Court. Therefore, these provisions should be removed from the Bill.

1.6. The Bill must mandate the notification of all personal data breaches to the DPA.

Section 25 (*Reporting of a personal data breach*) of the Bill deals with the reporting of a personal data breach. This section requires a data fiduciary makes a subjective assessment of whether a personal data breach is likely to cause harm, and only then send a notification to the DPA of the breach. Following this, the DPA must determine whether data principals should be notified of the breach (based on the severity of harm or if action is required on part of the data principal to mitigate such harm). For the reasons set out below, it is proposed that the data fiduciaries should mandatorily report all data breaches to the DPA and have the freedom to reach out to data principals where direct actions are required to protect themselves.

The positive effects of requiring the organisations to notify their data breaches can encourage them to implement higher security standards (Samuelson Law, Technology & Public Policy Clinic, 2007). This can further encourage market competition around security practices of data fiduciaries. Notifications should be recorded in a centralised, publicly available breach registry. This can enable better monitoring of the market, more research and analysis and improve supervisory capacities.

On the other hand, the process set up in section 25 could result in ineffective and limited breach notifications for several reasons. First, there is a lack of clarity on the definition of "harm". This makes it a poor trigger for such an obligation. This is especially problematic because it could create the wrong incentives for companies suffering breaches, who are now given an option of making a subjective decision of *whether* to report the breach. Second, the process also creates a bottleneck at the DPA, which may delay notification of a breach to data principals. This is especially worrying in cases where data fiduciaries need to inform data principals to take immediate action to protect themselves in the aftermath of a breach. Accordingly, it is submitted all data breaches should be reported to the DPA and

data fiduciaries should have the freedom to reach out to data principals where direct actions are required following a breach.

1.7. The Bill should strengthen obligations for data fiduciaries to incorporate Privacy by Design.

Section 22 (*Privacy by Design Policy*) of the Bill outlines the broad standards which should govern Privacy by Design (PbD) in India. It creates obligations for every data fiduciary to prepare a PbD policy that must be certified by the DPA. We note with concern that this obligation has been weakened compared to the previous draft of the Bill. Previously, the obligation on the data fiduciary was to implement policies and measures to ensure PbD principles were followed. In the new draft of the Bill, the obligation now is merely to prepare a PbD policy rather than implement PbD in all their practices and technical systems.

We welcome and appreciate these provisions on PbD which have become internationally recognized best practice in data regulation. However, the requirement in the previous draft of the Bill ensured better consumer data protection. In the current form, section 22 could limit the incentive on entities to internalise PbD principles to improve their working practices. Accordingly, the version of the provision included in the previous version of the Bill (at section 29) should be re-instated.

2. The Data Protection Authority has been weakened in the Bill, limiting the effectiveness of the new regime.

The design, powers and functions of the Data Protection Authority (DPA) have been considerably weakened in the Bill in comparison to the vision for the regulator in the previous draft of the Bill released in 2018.

2.1. Changes to the design and composition of the DPA diminishes its independence as a regulator.

It is important for the DPA to function as an independent regulator for it to regulate data processing activities effectively. It is well-established that choices about the organisational structure of a regulator can impact the regulators' overall behaviour and performance, including at the level of the individual employee (Carrigan & Poole, 2015). The composition and design of the management board is one of the key ingredients required to create an independent, accountable and impartial regulator. A management board must ensure a good mix of independent and government-appointed members, and the expected conduct of members must be laid out, with clearly identified requirements for accountability, including strict procedural requirements, reporting mechanisms and public consultation (Raghavan, Chugh, & Kumar, 2019). Unfortunately, changes in the Bill to the process for selecting the Chairperson and Members of the DPA risk compromising the quality of the future institution.

2.1.1. No independent Members are envisioned for the DPA

Section 42(1) of the Bill only foresees a Chairperson and six full-time Members as constituting the board of the DPA. In an emergent and fast-changing area like data protection regulation, it is important to have independent experts from technical and legal backgrounds to add perspective to the DPA's board. Having a board solely comprised of whole-time members could diminish the DPA's independence and ability to meet the challenges of regulating a dynamic field.

2.1.2. The Selection Committee of DPAs is now comprised entirely of Central Government bureaucrats

Under the previous draft of the Bill, the Selection Committee for the DPA was comprised of the Chief Justice of India (CJI) or another Judge of the Supreme Court, the Cabinet Secretary and a subject-matter expert appointed by the CJI and the Cabinet Secretary. This composition reflects the balance and robustness of views required to form a credible new regulator. Worryingly, this has been changed in the Bill with the result that the Selection Committee (described in section 42(2) of the Bill) consists only of Secretaries to the Central Government and its Ministries. This again, could diminish the DPA's independence and ability to meet the challenges of regulating a dynamic field.

The DPA envisioned by the Bill is a powerful body equipped with a range of enforcement tools including launch of investigations, levying civil penalties and criminal punishment. However, it does not have adequate internal accountability mechanisms to ensure that it uses its powers appropriately (Dvara Research, 2018b).[3] In the absence of adequate internal accountability measures, it becomes even more important that the DPA has regulatory independence without any conflict of interest so that its powers are not used arbitrarily. Rather than improving the accountability, transparency and effectiveness of the DPA, changes in the Bill could make the new body more opaque, unaccountable or ineffective.

We strongly recommend that the composition of the Selection Committee should be reversed to the previous formulation (i.e. Cabinet Secretary, Judge of the Supreme Court and an Independent Expert). The DPA should also mandate the requirement for four of the seven Members of the DPA to be independent Members.

[3] We highlighted the lack of adequate internal accountability mechanisms in our response to the draft Personal Data Protection Bill, 2018 (the draft Bill) which we published on 16 October 2018. We recommended that the design of the DPA include independent members as well as board-led governance that can impart greater accountability, transparency and legitimacy to the DPA's decisions. This recommendation is applicable to the present Personal Data Protection Bill, 2019 (the Bill) which has retained the design of the DPA under the draft Bill.

2.2. Substantive powers and functions of the DPA that have been removed should be re-allocated.

The Bill has removed some functions of the DPA that are important for effective regulation, and in some cases has re-allocated them to the Central Government.

2.2.1. The DPA no longer notifies additional "sensitive personal data"

Under the previous draft of the Bill, the DPA was empowered to notify additional categories of sensitive personal data. This power has now been shifted to the Central Government in section 15 of the Bill, for it to make such notifications in consultation with the DPA and relevant sectoral regulators. It is advisable for the DPA to retain this power, since it will be the regulator that is closest to the market with a day-to-day understanding of data practices that will enable it to make such a decision in consultation with its regulatory peers. The Central Government would not be well placed to make these decisions and could potentially delay regulatory response to new developments. Therefore, the DPA should retain the power to notify additional categories of sensitive personal data.

2.2.2. The DPA no longer has the exclusive power to notify significant data fiduciaries

Delegation of powers to bodies responsible for implementing the Bill must be done in a definitive and consistent manner in the governing legislation (Singh, 2004). However, there is an inconsistency in the delegation of powers between the Central Government and the DPA in determining and notifying significant data fiduciaries in the Bill.

The Bill empowers the Central Government to determine the threshold of users based on which social media intermediaries can be notified as significant data fiduciaries and notify them accordingly (in section 26(4)). This is inconsistent with the delegation of powers in the Bill which empowers the DPA to determine and notify significant data fiduciaries (in section 26(1)). The power to determine and notify social media intermediaries as significant data fiduciaries should be retained with the DPA to be consistent with the delegation of powers in the Bill.

We recommend that this power be retained with the DPA in consultation with the Central Government which can suggest social media intermediaries which should be considered in the interests of electoral democracy.

2.2.3. The DPA is no longer required to publish results of inspections and other comments in public interest

Under the previous draft of the Bill, the DPA had to publish results of any inspection or inquiry which it deems to be in public interest. This function has been omitted in the Bill. Publishing reports from inquiries and investigations promotes transparency in regulation which serves key interests of the regulator (Malyshev, 2008).

First, it helps the regulator serve user protection interests by informing data principals about the performance of relevant businesses (Financial Services Authority, 2008). Second, it can help relevant businesses in understanding the regulator's practices and refine internal procedures to comply with the law (Financial Services Authority, 2008). Third, it can create a feedback loop to help the regulator identify problems in the system and address them expeditiously (Dvara Research, 2018b). Fourth, it helps the regulator gain trust and legitimacy for their actions which is crucial for a regulator to be effective (Bertolini, 2006).

In context of the Bill, publishing results of inspections and investigations can help –

- data principals understand how different data fiduciaries are approaching data protection,
- data fiduciaries understand preferred practices to comply with the law,
- the DPA rectify problems in its rules and regulations, and
- afford more trust and legitimacy to the DPA's actions.

Accordingly, the provision at section 60(2)(w) in the previous Bill should be re-inserted to require the DPA to publish results of inspections and investigations in public interest.

3. Immense powers and exemptions for the State will severely limit the effectiveness of the new regime.

Section 35 of the Bill empowers the Central Government to pass orders to exempt itself or any other state agencies from any or all provisions of the proposed data protection regime. This provision is a dramatic shift from the exemption for the State provided in the earlier draft of the Bill (under that draft's section 42 (*Security of the State*)).

The new provision vastly expands the grounds of the exemption from "*interests of security of the State*" (in section 42 of the previous draft Personal Data Protection Bill 2018) to enabling the Central Government to pass orders whenever it considers it necessary or expedient in the interests of sovereignty and integrity of the country, national security, friendly relations with foreign states, public order or to prevent the incitement to commit offences that jeopardise these interests (see section 35(i) and (ii) of the new Bill). Simultaneously it removes the procedural and substantive safeguards that should exist for such exemptions to be claimed. Previously, the State exemption had to be used in "*accordance with the procedure established by such law, **made by Parliament** and is necessary for, and proportionate to, such interests being achieved* (emphasis added)" (see section 42(1) of the previous draft Personal Data Protection Bill 2018). The new section 35 empowers the Central Government to excuse State agencies from the requirements of the data protection law through executive orders. This offers wide discretion to the Central Government to abrogate the fundamental right to privacy via executive orders without any specific safeguards prescribed in the text of the Bill itself.

This provision poses many dangers to proposed Bill, including the risk of rendering it meaningless. If passed in its current form, this provision risks being challenged as unconstitutional. It is proposed that the formulation in section 42(1) of the previous version of the Bill should be re-instated and strengthened (including through judicial oversight mechanisms) to deliver meaningful data protection to the citizens of this country.

Puttaswamy's three-part test for any law seeking to restrict the right to privacy

The Supreme Court in K.S. Puttaswamy v Union of India, (2017) (*Puttaswamy*) upheld the right to privacy as a fundamental right in India, recognising it as an inalienable human right predating the constitution itself. The lead judgment located the right to privacy across various provisions of Part III of the Constitution including Articles 14, 19 and 21. Like other fundamental rights, the right to privacy can be subject to reasonable restrictions provided that such restrictions fulfil the conditions set out in the Constitution. Specifically, the lead judgment in *Puttaswamy* set out a three-part test that any restriction to the right to privacy should meet to be considered reasonable i.e. (para 180, *Puttaswamy*):

(i) the existence of a law i.e. an action of the Central Government to limit the right to privacy needs to be backed by a law. This requirement arises from the content and procedural mandates of Article 21 of the Constitution, that requires that any action that deprives a person of their right to liberty must be backed by a law;

(ii) legitimacy i.e. the Central Government must restrict the right to privacy only to satisfy a legitimate state aim, and

(iii) proportionality i.e. the quality and severity of restrictions on privacy must match the objective of the law. The means to curtail privacy, adopted by the legislature should not be disproportionate to the objectives of the law.

While setting out this test, it was clarified in the lead judgement that the three-part test emanated from the procedural and content-based mandates of Article 21. Under Article 21, it is established jurisprudence that any procedure established by law to restrict fundamental rights should be reasonable, just and fair and it should be free from any unreasonableness and arbitrariness (*Maneka Gandhi vs Union Of India*, AIR 1978 SC 597). In addition, *Puttaswamy* also called out that restricting rights for a "legitimate" state aim automatically required such law to fall within the zone of reasonableness mandated by Article 14 i.e. it must not be arbitrary.

Given this context, section 35 in its current form could potentially be challenged as falling short of the *Puttaswamy* test, as well as the content and procedure-based conditions in the Constitution for restricting rights under Articles 21, 19 and 14.

3.1. The wide powers delegated through section 35 without clear guidance and safeguards on its use opens it up to constitutional challenge.

Section 35 provides a wide variety of grounds for Central Government to act to restrict privacy, without clearly specifying and confining the bounds within which such power can be exercised. The outcome of the *Puttaswamy* constitutional court decision was to highlight the role of the legislature in giving effect to the entitlements in the Constitution. It should aim to do so, by setting out more substance and guidance on how the Central Government must use any power delegated to it—rather than delegating its own role to the Central Government.

The vastness of the power delegated in section 35 make it difficult to understand if a legitimate or proportionate objective is being fulfilled when delegated legislation is made under this provision. This could open up the provision to challenges of arbitrariness since it fails to provide clear and specific safeguards to guarantee against arbitrary state action. Instead, section 35 merely states that the very Central Government official passing orders to abrogate citizens' privacy will decide what "*procedure, safeguards and oversight mechanism*" should be followed (see section 35). Other approaches such as setting out the conditions for exercise of power (such as in section 42 of the previous version of the Bill), or the use of judicial oversight mechanisms are clearly better alternatives to ensure legitimacy and proportionality of this provision, and to ensure it is not adjudged to be arbitrary overall.

It is well recognised that to be reasonable and non-arbitrary, any Act needs to lay down policy and guidelines for exercise of power while conferring arbitrary powers on the executive (*State of W.B. v Anwar Ali Sarkar* (AIR 1952 SC 75)). The Supreme Court has also held in *The Special Courts Bill, 1978 Re* (AIR 1979 SC 478) that a law must provide a clear and definite legislative policy in order to be reasonable.

The wideness of the powers and absence of clear safeguards to guide their use by the Central Government Authorities to whom they are delegated, is especially worrying since section 35 enables a simple executive order to be passed to abrogate fundamental rights of citizens. As noted in the *Puttaswamy* judgement, and the subsequent judgement on the constitutionality of Aadhaar in *K.S.Puttaswamy (Retd) vs Union of India,* (2019) 1 SCC 1 (Puttaswamy II):

> "*Nine judges of this Court in Puttaswamy categorically held that there must be a valid law in existence to encroach upon the right to privacy. An executive notification does not satisfy the requirement of a valid law contemplated in Puttaswamy. A valid law, in this case, would mean a law enacted by Parliament, which is just, fair and reasonable. Any encroachment upon the fundamental right to privacy cannot be sustained by an executive notification*."

The absence of clear guidance and safeguards to fetter and guide the Central Government's power to exercise in section 35 will require the Central Government to take on the mantle of making its own

unfettered determination as to legitimacy, proportionality, procedure, safeguards and oversight mechanisms. The intent of the legislature in giving voice to our fundamental rights in this Bill must be to uphold them and provide careful guidance and safeguards when they are restricted, rather than to abdicate this function in favour of some outside authority (Singh, 2019, pp. 1043-48).

Accordingly, it is proposed that the formulation in section 42(1) of the previous version of the Bill should be re-instated and strengthened (including through judicial oversight mechanisms) to deliver meaningful data protection to the citizens of this country.

4. The Bill should strengthen consumer protections within the proposed sandbox and clarify its objectives.

Section 40 (*Sandbox for encouraging innovation, etc.*) of the Bill envisages a sandbox "*for innovation in artificial intelligence, machine-learning or any other emerging technology in public interest*". We welcome the attempt to support innovation and prepare regulation for emerging technology. However, we have serious concerns on the user protection afforded in this provision. In its current form, the provision also does not clarify the rationale and objectives for creating the sandbox. It is important to include these in the primary legislation to ensure that the future development of the sandbox is safe and structured.

4.1. Consumer protection safeguards are completely absent in section 40.

Section 40(4)(c) (*Sandbox for encouraging innovation, etc.*) removes obligations for entities in the sandbox to adhere to certain user protections in Chapter II of the Bill i.e. specify purpose of data collection, and the limitations on the collection and storage of personal data. This could mean a data fiduciary that is accepted into the sandbox is either not bound by the obligations in the Bill or is bound by modified and diluted forms of these obligations. This blanket vacation of consumer protections, instead of the *addition* of consumer protections is uncommon and should be rectified.

We are very concerned that this can expose individuals to risks. Entities participating in a sandbox perform experimental operations on personal data of individuals, effects of which may not be immediately understood and could expose users to new risks. In these circumstances, it is important to enhance users' understanding of their interaction with a "sandboxed" entity rather than keep them in the dark or dilute their protections. We note that the emphasis on the need to notify test customers of potential risks, available compensation and to obtain their explicit consent regarding the testing is part of the RBI's Enabling Framework for Regulatory Sandbox in section 6.8 (*Consumer Protection*). It is also repeatedly emphasised that upfront liability for consumer will lie with the sandbox participant, and that its entry into sandbox does not in any way limit an entity's liability towards its customers (Reserve Bank of India, 2019a).

Section 40 must clearly set out the additional protections for individuals that are common in sandbox frameworks around the world and in India. It must ensure data principals' rights are extended rather than curtailed in the sandbox, that clear redress mechanisms are specified and that all participants ensure that all obligations towards customers are fulfilled before they exit the sandbox. The sandbox must strengthen rather than remove data principals' protections when they are interacting with entities that are sandbox participants.

4.2. The objectives of the sandbox are unclear which could result in overlaps with other sandbox efforts (such as the RBI Sandbox).

The objectives for creating the sandbox in section 40 broadly refers to supporting innovation for "public interest". Vagueness in the objectives could create a situation where regulators are unable to assess the feasibility, potential outcomes and collateral effects of operations in the sandbox (UNSGSA, 2019). It also creates uncertainty when assessing the interaction with other regulators and sandboxes (Madi, 2019). This is especially important since India already has a live sandbox. The proposed sandbox under the DPA may overlap with the RBI's fintech sandbox which began operation in November 2019 (Reserve Bank of India, 2019b). This can create risks of regulatory arbitrage or over-regulation if regulatory perimeters are not clearly defined. For instance, certain fintech applications could be using AI, ML or other emerging technologies. Would they need to pass through both the DPA's and the RBI's sandbox? A clearer articulation of the objectives of a sandbox in the Bill will help the DPA frame narrower and aligned objectives as it operationalises the sandbox. One example is available in the US, where the creation of the sandbox, Project Catalyst by the Consumer Financial Protection Bureau (CFPB) was informed by the objective in its governing statute (Dodd Frank Wall Street Reform and Consumer Protection Act 2010) (Consumer Financial Protection Bureau, 2016) i.e.

> "*to ensure that the markets for consumer financial products and services operate efficiently and transparently to facilitate access and innovation".*

This objective pins the support for innovation to a specific outcome i.e. efficiency and transparency of markets for retail financial products. This helps clarify the mandate of the particular sandbox. It is recommended that the Bill clearly articulate the objectives and sub-objectives which can inform the DPA while scope and design of the proposed sandbox (Raghavan, Chugh, & Singh, 2019).

5. "Harm" should not be a condition on which rights and obligations depend in the Bill.

Section 3(20) of the Bill sets out a very broad definition of "harm". This definition is a compilation of 10 adverse outcomes with no discernible links to each other or to a misuse of personal data. Further, the provision does not offer any conceptual framework or guidance to explain how to interpret the list of outcomes or the relationship between the different types of outcomes on the list (Dvara Research,

2018b). Despite this, twenty-three significant provisions in the Bill are contingent on the occurrence of "harm" of which (Ministry of Electronics and Information Technology, 2019)–

- 3 provisions relate to the exercise of their rights by data principals and access grievance redress forums.[4]
- 9 provisions relate to the fulfillment of data protection obligations by data fiduciaries.[5]
- 11 provisions relate to the enforcement of the Bill by the Central Government and the DPA.[6]

This treatment of harm in the Bill can compromise consumer protection, business certainty and effective regulation. A thorough analysis of the definition of harm shows that the list-based definition is vague and appears unconnected to misuse of personal data. It does not offer a framework that consumers, providers and regulators can refer to for identifying and quantifying harm. It is also unclear about new harms that can arise as technology evolves (Prasad, 2019) (Dvara Research, 2018b). This leaves the interpretation of harm to the subjective assessment of consumers, providers and regulators, severely weakening the regulatory regime proposed by the Bill (Dvara Research, 2018b) (Prasad, 2019). This ambiguity across stakeholders makes it difficult to identify a harm and attribute damage to it. Therefore, it is very problematic to link the fulfilment of rights and obligations with the occurrence of harm given the nature of its definition in the Bill.

Accordingly, it is submitted that "harm" **<u>should not be a condition</u>** on which rights and obligations depend in the Bill. These rights and obligations should be fulfilled irrespective of the occurrence of harm.

In addition, a broader definition of harm should be included in the Bill together with a broad obligation on providers to take reasonable efforts to avoid causing harm (Dvara Research, 2018b). A definition of harm that could be used for this purpose is (Dvara Research, 2018a):

> *""harm" is actual or potential injury or loss to an individual, whether such injury or loss is economic or non-economic, quantifiable or non-quantifiable."*

[4] *See* provisions on "*General conditions for the exercise of rights in this chapter*" (section 21(5)), "*Grievance redressal by data fiduciary*" (section 32(2)) and "*Compensation*" (section 64(1)).
[5] *See* provisions on "*Processing of personal data and sensitive personal data of children*" (section 16(3) & section 16(5)), "*Privacy by design policy*" (section 22(1)(a)), "*Transparency in processing of personal data*" (section 23(1)(c)), "*Security safeguards*" (section 24(1)), "*Reporting of personal data breach*" (section 25(1) & section 25(3)), "*Data protection impact assessment*" (section 27(1) and section 27(3)(b)),
[6] *See* provisions on "*Categorisation of personal data as sensitive personal data*" (section 15(1)(a) & section 15(1)(c)), "*Reporting of personal data breach*" (section 25(5)), "*Classification of data fiduciaries as significant data fiduciaries*" (section 26(1)(d), section 26(1)(f) and section 26(3)), "*Data protection impact assessment*" (section 27(5)), "*Audit of policies and conduct of processing etc*" (section 29(7)), "*Conditions for transfer of sensitive personal data and critical personal data*" (section 34(1)(a)(ii)), "*Exemption for research, archival or statistical purposes*" (section 38(e)), "*Procedure for adjudication by Adjudicating Officer*" (section 63(3)).

6. The Bill should not include provisions relating to the sharing of Non-Personal Data.

Three new provisions of the Bill relate to anonymised data and non-personal data, which otherwise falls entirely outside the ambit of this Bill. These provisions are sections 91(2), 91(3) and a portion of section 2(B). The effect of these provisions is to selectively include powers in the Bill for Central Government to direct firms to hand over anonymised or non-personal data sets to the Government for its use in service delivery and policy-making.

Section 91(2) of the Bill gives the Central Government the power to direct any data fiduciary or data processor to provide any non-personal data to it. Such directions may be made in consultation with the DPA. The stated objective for such directions will be "*to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government*". Section 91(3) mandates the disclosures of such directions made by Central Government annually. Section 2(B) of the Bill states that the application of this statute will not extend to anonymised data, other than in the case of anonymised data in section 91.

It is humbly submitted that provisions relating to non-personal data should be omitted from this Bill for the reasons set out below.

6.1. Provisions unrelated to the objectives of personal data protection should not be included in the Bill.

The provisions in the Bill should be in furtherance of the overarching intention and objectives of the Legislature for proposing the Bill. The clear objective of the Bill is to empower citizens with rights relating to their personal data and ensure their fundamental right to privacy. Section 91(2) and (3) and the portion of section 2(B) that selectively extends the applicability of the Bill to anonymised data, do not relate to this objective. Their inclusion is not in keeping with the arrangement and logic of the Bill.

It is a compelling and settled rule that statutes must be read as a whole and in their context (Singh, 2016). Every clause in any law passed by Parliament needs to be construed with reference to context and the other clauses, to ensure there is a consistent enactment of the statute relating to a particular subject matter (Singh, 2016).

The primary and core focus on the protection of personal data in the Bill is clear from its context and its bare text. This focus was recognised by the Government when constituting the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna to suggest a draft Bill (Government of India, 2017). Personal data and privacy were consistently identified in the Committee's White Paper and Final Report, coming as they did in the background of the Supreme Court's specific acknowledgement in the *Puttaswamy* matter that the Committee had been constituted by the Government of India to suggest an Indian regime for data protection and to protect informational privacy of individuals (Justice K.S.

Puttaswamy (Retd) & Anr vs Union of India & Ors., 2017). The Title, Preamble, Headings and Statement of Objects and Reasons of the Bill reiterate this focus on personal data protection.

Therefore, the entire context of the Bill makes it clear that it is aimed to create a framework for personal data. Non-personal data or anonymised data is by their very definition in the Bill separate and distinct from personal data. Any regulatory framework seeking to deal with such non-personal data will be driven by a range of objectives and needs that are not related to the regulation of personal data. Consequently, the provisions relating to anonymised and non-personal data in sections 91(2), 91(3) and 2(B) should not be part of the Bill.

6.2. Policy and regulation of non-personal data (if any) should be dealt with independently and separately from the draft Bill.

A range of objectives could drive any future policy or regulation on non-personal data, such as ensuring competitiveness of firms, or developing India's international trade and commerce in a digital economy, or national security (Singh, Raghavan, Chugh, & Prasad, 2019). Other objectives could include considering the interests of communities or groups in their data could be collectively safeguarded, or how a country's anonymised data could be tapped as a community or public resource (Government of India, 2019). Such objectives might very well be legitimate, but as such have no place in a law dealing with personal data protection.

Data protection laws are specifically aimed at regulating the processing of individual natural/physical persons, and primary formal objective of such laws is to safeguard the privacy-related interests of those persons (Bygrave, 2014). These objectives would have limited (if any) application for dealing with data that is anonymised or "non-personal". The sole concern for a data protection law or a future DPA could be in relation to mitigating privacy risks from re-identification of individuals from anonymised data sets. The Government of India has already recognised this disparity, as is evident from the setting up of the separate Committee to study various issues relating to non-personal data in September 2019 (Government of India, 2019). Any laws or regulations relating to anonymised or non-personal data should emerge as a part of that Committee's process, rather than be included in the draft Personal Data Protection Bill which has fundamentally different aims and objectives.

6.3. Other complications arise if provisions relating to non-personal data are included in the Bill.

The internal logic of the draft Bill does not accommodate these three provisions on non-personal data.

6.3.1. Entities cease to be data fiduciaries or data processors when dealing with anonymised data

The definition of "data fiduciary" and "data processor" in the Bill only relates to entities connected with the processing of personal data. The moment the data being processed becomes anonymised or non-personal data, then entities cease to be "data fiduciaries" or "data processors" under this Bill.

Consequently, it appears that it would be a logical impossibility for Central Government to make such directions.

6.3.2. The involvement of the DPA in passing such directions conflicts with its mandate in the Bill

Section 91(2) foresees the Central Government consulting with the DPA in order to direct the handing over of non-personal data to the Government. The primary objective of a future DPA will be to protect the interests of data principals and prevent the misuse of personal data (*see* section 49 of the Bill). Across the world, almost every country with a comprehensive statutory framework for data protection establishes a specialised agency to oversee the implementation of data privacy regimes, handle complaints, give advice and raise public awareness regarding data privacy issues (Bygrave, 2014). Muddling these objectives and functions by adding discrete provisions dealing with non-personal data could dilute the DPA's focus on privacy, and potentially require it to engage with an issue otherwise outside its knowledge and competence.

For the reasons set out above, it is submitted that section 91(2) and 91(3) should be removed from the draft Bill. The words "*other than the anonymised data referred to in section 91*" should also be removed from section 2(B).

7. The Bill should contain transitional provisions to create certainty about its implementation.

The previous draft of the Bill set out transitional provisions in section 97. These provisions set out the maximum time that the Government can take in enacting the provisions of the Act from the date it is passed in the Parliament. Further it set out the timelines for establishing the DPA and gradually implementing most provisions of the Act within 30 months of the enactment (Prasad, Raghavan, Chugh, & Singh, 2019).

The Personal Data Protection Bill 2019 does not have a comparable provision. Therefore, there is no clarity on the path to implanting the data protection regime after the Bill is passed in the Parliament.

The absence of any time frames for enforcement of the provisions of the Act creates sizeable uncertainty for data processors and data fiduciaries. In its current form, it is difficult to interpret if all the provisions of the Act come into force on the date of the enactment itself or over a longer time period. This does not give data fiduciaries and data processors clarity on the time horizon to update their policies and processes. They may not be able to honour the obligations of the Act in a timely fashion. Our analysis suggests that the Personal Data Protection Bill of 2018 triggered close to 100 action points for data fiduciaries and data processors (Prasad, Raghavan, Chugh, & Singh, 2019). This Bill is likely to have similar effects.

On the flip side, silence on time frames for enforcing the provisions of the Bill may also adversely affect how much teeth it has in practice. In the absence of clear sunset and sunrise provisions in the Bill, there could be neither political will nor industry support to bring the enforcement architecture of the Bill into effect. The likelihood of this scenario is overwhelming, considering India's experience with the Information Technology Act, 2000. The Act was amended in 2008 to include requirements for reasonable security practices and procedures in relation to personal data processing, but Rules to bring these into effect were not passed until 2011, and enforcement and grievance redress institutions were not notified for many years afterwards (Greenleaf, 2014).

This has a direct impact on individuals' fundamental right to privacy. Data principals may find themselves in a precarious situation where their rights in relation to their personal data have been upheld by the Parliament but there is no effective machinery to enforce them or remedy contraventions in relation to them. Thus, the absence of time frames could have the effect of a constitutional guarantee not being given effect by the legislature and limiting individuals' right to privacy to an academic notion.

It is therefore imperative to offer some timeframes for when the different provisions and aspects of the Bill shall come into force.

References

Samuelson Law, Technology & Public Policy Clinic. (2007, December). *Security Breach Notification Laws: Views from Chief Security Officers.* Retrieved January 2020, from University of California, Berkeley: https://www.law.berkeley.edu/files/cso_study.pdf

Bertolini, L. (2006, June). *How to improve regulatory transparency: Emerging lessons from an international assessment.* Retrieved from PPIAF: https://ppiaf.org/documents/3005?ref_site=ppiaf&keys=how%20to%20improve%20regulatory%20transparency&restrict_documents=false&restrict_pages=true&site_source%5B%5D=PPIAF

Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective.* New York, United States of America: Oxford University Press.

Carrigan, C., & Poole, L. (2015, June). Structuring Regulators:The Effects of Organizational Design on Regulatory Behavior and Performance. *Penn Program on Regulation* . Philadelphia, Pennsylvania, United States of America. Retrieved from https://www.law.upenn.edu/live/files/4707-carriganpoole-ppr-researchpaper062015pdf

CGAP, Dalberg & Dvara Research. (2017, November). *Privacy on the Line.* Retrieved January 2020, from Dvara Research: https://www.dvara.com/research/wp-content/uploads/2017/11/Privacy-On-The-Line.pdf

Consumer Financial Protection Bureau. (2016, October). *Project Catalyst report: Promoting consumer-friendly innovation.* Retrieved from Consumer Financial Protection Bureau: https://files.consumerfinance.gov/f/documents/102016_cfpb_Project_Catalyst_Report.pdf

Dvara Research. (2018a, February 7). *The Data Protection Bill, 2018.* Retrieved from Dvara Research: https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf

Dvara Research. (2018b, October 10). *Comments to the Ministry of Electronics and Information Technology (MEITy) on the draft Personal Data Protection Bill 2018, dated 27 July 2018, submitted by the Committee of Experts on a Data Protection Framework for India.* Retrieved from Dvara Research: https://www.dvara.com/blog/wp-content/uploads/2018/10/Response-to-draft-Personal-Data-Protection-Bill_DvaraResearch.pdf

European Union. (retrieved in 2020). *Recital 68: Right of Data Portability*. Retrieved from EU GDPR: https://gdpr-info.eu/recitals/no-68/

Financial Services Authority. (2008, May). *Transparency as a Regulatory Tool.* Retrieved from Financial Services Authority: https://www.fca.org.uk/publication/discussion/fsa-dp08-03.pdf

Government of India. (2017, July 31). *No. 3(6)/ 2017-CLES Office Memorandum: Constitution of a Committee of Experts to deliberate on a data protection framework for India.* Retrieved January 2020, from Ministry of Electronics & Information Technology: https://meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf

Government of India. (2019, September 13). *No. 24(4) /2019-CLES Office Memorandum: Constitution of a Committee of Experts to deliberate on Data Governance Framework.* Retrieved January 2020, from Ministry of Electronics & Information Technology:

https://meity.gov.in/writereaddata/files/constitution_of_committee_of_experts_to_deliberate_on_data_governance_framework.pdf

Greenleaf, G. (2014). *India's data protection impasse: Conflict at all levels, privacy absent*. Retrieved from SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2438366

Justice K.S. Puttaswamy (Retd) & Anr v. Union of India & Ors, W.P (Civil) No 494 of 2012 (The Supreme Court of India September 26, 2018). Retrieved from https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

Justice K.S. Puttaswamy (Retd) & Anr vs Union of India & Ors., W.P. (Civil) No. 494 of 2012 (The Supreme Court of India August 24, 2017). Retrieved from https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

Madi, J. (2019). *FinTech: Law and Regulation.* Edward Elgar Publishing. Retrieved from https://books.google.co.in/books?id=2j6tDwAAQBAJ&pg=PA322&lpg=PA322&dq=Objective+of+sandboxes+should+be+clear&source=bl&ots=W-GWMnZ43g&sig=ACfU3U0zl3a69Haah-eocDhKA8zpHCF4KA&hl=en&sa=X&ved=2ahUKEwiu2JakqIDnAhUYWCsKHXUyDVwQ6AEwEXoECAoQAQ#v=onepage&q=Object

Malyshev, N. (2008). *The Evolution of Regulatory Policy in OECD Countries.* Retrieved from OECD: https://www.oecd.org/gov/regulatory-policy/41882845.pdf

Ministry of Electronics and Information Technology. (2019, December 11). *Personal Data Protection Bill, 2019.* Retrieved from PRS Legislative Research: http://prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf

Narayanan, A., & Shmatikov, V. (2008). Robust De-anonymisation of large datasets. *2008 IEEE Symposium on Security and Privacy* (pp. 111-125). Washington DC: IEEE Computer Society. Retrieved August 23, 2018, from https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

Prasad, S. (2019, October 29). *An Analysis of 'Harm' defined under the draft Personal Data Protection Bill, 2018*. Retrieved from Dvara Research: https://www.dvara.com/blog/2019/10/29/an-analysis-of-harm-defined-under-the-draft-personal-data-protection-bill-2018/

Prasad, S., Raghavan, M., Chugh , B., & Singh, A. (2019, October). *Implementing the Personal Data Protection Bill: Mapping Points of Action for Central Government and the future Data Protection Authority in India*. Retrieved from Dvara Research Blog: https://www.dvara.com/blog/2019/10/03/implementing-the-personal-data-protection-bill-mapping-points-of-action-for-central-government-and-the-future-data-protection-authority-in-india/

Raghavan, M., Chugh, B., & Kumar, N. (2019, November). *Effective Enforcement of a Data Protection Regime*. Retrieved January 2020, from https://www.dvara.com/research/wp-content/uploads/2019/12/Effective-Enforcement-of-a-Data-Protection-Regime.pdf

Raghavan, M., Chugh, B., & Singh, A. (2019, May 8). *Comments to the Reserve Bank of India (RBI) on the Draft Enabling Framework for Regulatory Sandbox dated 18 April 2019 (the Draft Framework).* Retrieved from Dvara Research: https://www.dvara.com/blog/2019/05/08/our-response-to-the-reserve-bank-of-india-on-the-draft-enabling-framework-for-regulatory-sandbox/

Rao, G. (2003). *Special Contracts (Law of Contract II).* Hyderabad: S. Gogia & Company.

Reserve Bank of India. (2019a, August 13). *Enabling Framework for Regulatory Sandbox.* Retrieved from Reserve Bank of India: https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=938

Reserve Bank of India. (2019b, November 4). *Reserve Bank announces the opening of first cohort under the Regulatory Sandbox.* Retrieved January 2020, from Reserve Bank of India: https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=48550

Singh, A., Raghavan, M., Chugh, B., & Prasad, S. (2019, September 24). *The Contours of Public Policy for Non-Personal Data Flows in India.* Retrieved January 2020, from Dvara Research Blog: https://www.dvara.com/blog/2019/09/24/the-contours-of-public-policy-for-non-personal-data-flows-in-india/

Singh, J. G. (2016). *Principles of Statutory Interpretation.* Gurgaon, Haryana, India: LexisNexis.

Singh, M. P. (2004). *V.N. Shukla's Constitution of India Tenth Edition.* New Delhi: Eastern Book Company.

The Constituent Assembly of India. (1950). *The Constitution of India.* Retrieved from National Portal of India: https://www.india.gov.in/sites/upload_files/npi/files/coi_part_full.pdf

The World Bank. (2018). *GDP per capita, PPP (current international $)*. Retrieved from The World Bank: https://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD?view=chart

UNSGSA. (2019). *Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech.* Retrieved from UNSGSA: https://www.unsgsa.org/files/2915/5016/4448/Early_Lessons_on_Regulatory_Innovations_to_Enable_Inclusive_FinTech.pdf