Comments to the Joint Parliamentary Committee (JPC) 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 comments on the Personal Data Protection Bill 2019 (the **Bill**), introduced in the Lok Sabha in December 2019, and referred to the JPC on the Bill. Our feedback on the Bill is presented in this document in two sections.

Section I presents seven overarching concerns with the Bill (set out below), with detailed analysis and recommendations to address these concerns constructively.

1. User protections must be strengthened for the Bill to genuinely guarantee data privacy for Indians.
2. Changes to the institutional design of the DPA could limit its independence, accountability and effectiveness.
3. Immense powers and exemptions for the State will severely limit the effectiveness of the new regime.
4. Fair and reasonable processing should be an overarching obligation on data fiduciaries and data processors
5. "Harm" should not be 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.

Section II presents a comprehensive Chapter-wise analysis of the provisions of the Bill against the previous draft Personal Data Protection Bill, 2018 (the **previous Bill**), flagging new issues arising from changes as well as persisting concerns.

This response continues our engagement with the public consultation process on India's new data protection regime since 2017.[2] 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.

We urge the JPC to engage with our recommendations to create an effective, consumer-friendly data protection framework for India's unique context. We welcome any opportunity to present these views or respond to questions and comments on our research to the JPC.

[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 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 Expert Committee on Data Protection 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.

CONTENTS

SECTION I: OVERARCHING COMMENTS

In this section, we highlight seven pressing concerns in the Bill, along with proposals and recommendations to address these concerns.

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

Several aspects of user protection that are weakened in the latest draft of the Bill are outlined below. These specific protections must be strengthened for a framework that seeks to protect and serve Indian citizens. Taken together, they weaken obligations to provide notice when users' data is collected, constrain the rights of users, limit user protections afforded by breach notifications and dilute Privacy by Design obligations for data fiduciaries.

1.1. The Bill should not remove obligations to give notice to individuals for non-consensual processing of their personal data.

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 requirement to give notice (even for non-consensual processing) has now been introduced in the Bill. As per section 7(3) (*Requirement of notice for collection or processing of personal data)*, providers need not give notice to individuals whose personal data they are processing where it would "*substantially prejudice"* the purpose of processing on *any* of the non-consensual grounds allowed in the Bill. 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.

Further, the requirement to give notice may also be removed by the DPA when data is processed non-consensually for "reasonable purpose" under section 14(3)(b) (*Processing of personal data for other reasonable purposes*).

It is submitted that obligations to provide notice to users should be reinstated in the Bill. Exemptions from the need to serve notice should be limited only to cases of severe emergency (as was the case in the previous version of the Bill). If not, it could increase opacity in the operations of data fiduciaries for non-consensual data processing activities, creating a complete information asymmetry between the data fiduciary and the data principal. This would directly and adversely affect users' ability to assess how

their data is being used and identify contraventions in the processing of their data. It could severely limit 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 she does not have a "valid reason" for withdrawal. We submit that 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 of consent 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 the Dvara Bill (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 Data Protection Authority (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 its 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, and also allow data fiduciaries to notify users directly

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 to make 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 recognised 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. Changes to the institutional design of the DPA could limit its independence, accountability and effectiveness.

The design, powers and functions of the DPA have been considerably weakened in the Bill in comparison to the vision for the regulator in the previous Bill. The lack of certain well-recognised

design features could result in a DPA that is not functionally independent, and could act arbitrarily, raising the potential for abuse of the DPA's powers. These concerns are set out in greater detail below.

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).

2.1. Changes to the design and composition of the DPA's Management Board weaken its independence

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. Further, the provision does not specify the minimum number of Members should be that should be appointed to the DPA.

Specifically, the provision:

- **Allows for under-staffing of the DPA:** The provision prescribes that the DPA cannot appoint more than 6 whole time members. We submit that by not prescribing the minimum number of members to be appointed into the DPA, the provision could have the effect of the DPA being severely understaffed. This could limit its ability to effectively discharge its regulatory obligations as set out under the Act.
- **Precludes the appointment of independent members:** The lack of independent members in the DPA, significantly departs from the governance structure of established Indian regulators such as the RBI, the SEBI and well-established principles of regulatory design. The inclusion of independent or non-executive members is seen as an important fetter on the discretionary power of the whole-time members serving the regulator. Independent members are expected to act as neutral

observers and hold the regulator accountable (Government of India, 2013). Independent members with technical expertise can also be valuable resources for the regulator to help it make informed decisions and further public interest (OECD, 2014). A good mix of independent and government-appointed members on the Board, further engrains collegiality which also ensures diversity in opinions and offers resistance against regulatory capture (Raghavan, Chugh, & Kumar, 2019).

It is noted that the comparable provision in the previous Bill (section 50(1)) merely stated that the DPA should consist of a Chairperson and 6 whole time members, leaving open the possibility to appoint Independent Members.

Accordingly, it is submitted the Bill should mandate that the Management Board of the DPA is dominated by Independent Members. This is in line with well-established principles of institutional design (Roy, Shah, Srikrishna, & Sundaresan, 2019). Ideally, there should be a requirement for four of the seven Members of the DPA to be independent Members.

2.1.2. The Selection Committee of DPA 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 could diminish the DPA's independence and ability to meet the challenges of regulating a fast-changing field. It is important to draw from technical and legal expertise, knowledge and networks when staffing a regulator that will need to be dynamic and up to date with current practices in data processing, data science and related regulatory thinking.

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).

2.1.3. The DPA is bound by Central Government's directions when exercising its powers and functions

The weaknesses in the composition and selection process of the Management Board of the DPA are compounded by another provision that could further undermine the independence of the DPA. Section 86 (*Power of Central Government to issue directions*) empowers Central Government to issue directions to the DPA which it will be bound by when exercising any powers or discharging functions. This provision does not mandate prior consultation or consensus to be achieved with the DPA and

merely states that the DPA "*shall, as far as practicable, be given an opportunity to express its views*" before a direction is given.

Within the context of the weaknesses of the DPA's institutional design in the Bill, this provision further erodes the independence of the DPA and exposes it to undue governmental interference. An important dimension of a regulator's independence is their independence from politics, i.e. independence from governments, parliaments, parties and individual politicians (Koop & Hanretty, 2017; Hanretty & Koop, 2012). Further, a significant indicator of political independence of regulatory agencies is the degree of independence conferred in them by the legal instruments that create and govern these agencies (Hanretty & Koop, 2012). This provision therefore further exposes the DPA to interference from the Central Government, compromising its ability to act independently.

In the realm of data protection, the independence of supervisory agencies has become the cornerstone of several DPAs established around the world. Art 52 (*Independence*) of the GDPR mandates that all EU DPAs should "*act with complete independence*" when performing their tasks. Decisions of the Court of Justice of the European Union have noted that the mere risk that other authorities can exert political influence over the decisions of such supervisory DPAs hinders the independent performance of the DPA's tasks (European Commission v Federal Republic of Germany, 2010). Even outside the EU, the well-recognised OECD Privacy Guidelines have highlighted the need for independence of DPAs in a manner free from influence that compromises their professional judgment, objectivity or integrity (OECD, 2013, p. 28).

To fulfil the vision for a truly independent DPA, it is important to ensure that the DPA's functional independence is not overridden by the directions and diktats of the Central Government. Apart from setting back interests of Indian data principals, these matters could also adversely impact India's 'adequacy' determination under the GDPR. In order to receive and process European personal data, India will need to be deemed "adequate" under Art 45 of the GDPR (Art. 45: Transfers on the basis of an adequacy decision, 2015). Effective and independent supervision of data protection is an important parameter for countries to be determined as 'adequate' under Art. 45 of the EU GDPR (EU GDPR, 2015). The design features that limit the independence of the DPA outlined in this section could result in India's adequacy determination becoming untenable, thereby also restricting the ability of Indian industry to provide services to European markets.

2.2. The absence of crucial accountability mechanisms can enable a future DPA to act arbitrarily or abuse powers.

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). In the absence of adequate internal accountability measures, it becomes even more important that the Bill incorporates key accountability mechanisms when establishing the DPA to ensure its powers are not used arbitrarily.

Unfortunately, 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.

2.2.1. The Bill must include discretion-fettering provisions to guide the extensive enforcement powers of the DPA.

The DPA envisioned in the Bill has access to a range of enforcement tools, from issuing softer warnings and reprimands, to full blown investigations that can lead to severe penalties and even criminal punishment. To ensure that these punitive powers are not abused and misused, there is a need to create clear mechanisms that guide and fetter the DPA's discretion (Raghavan, 2020). Setting out objective criteria to guide such discretion will also result in responsive regulation, that can more cheaply crowd in the rule of law orientation among newly-regulated entities in a vast regulated space. The theory (and practice) of Responsive Regulation calls for a measured and transparent escalation of sanctions, from softer enforcement tools to harder actions for entities that infringe any regime (Ayers & Braithwaite, 1992). Given the credible threat of punitive action, the regulator can then use softer (and less costly) enforcement actions more regularly, conserving regulatory capacity which is precious in a context like India (Raghavan, Chugh, & Kumar, 2019).

In a mock legislative instrument developed to support Dvara Research's response to the White Paper of the Committee of Experts, specific statutory clauses that could be used to create such fettering were suggested (the Dvara Bill) (Dvara Research, 2018a). These clauses extracted in Box 1 below) require:

- any enforcement action authorised by the DPA to be proportionate to the relevant contravention; and
- specific factors to drive the choice of enforcement tool by the DPA, such as the nature and seriousness of the contravention, the consequences of the contravention e.g. the unfair advantage gained, loss or harm caused, repetitive nature of the contravention etc.

Including the language in Box 1 in the Bill will be an important part of ensuring it plays a credible and legitimate role to uphold the interests of data principals (Raghavan, 2020). This plays an important role in signalling the credibility of a regulator. This has been seen in India's regulatory experience, with respect to the Telecom Regulatory Authority of India (TRAI). TRAI has consistently been a more consultative and transparent regulator—and held to account in judicial and quasi-judicial proceedings to be transparent—as one of the few Indian regulators with an explicit requirement to be transparent in its actions in section 11(4) of the TRAI Act (Krishnan & Burman, 2019).

Box 1: Fettering the DPA's Discretion
Extract from section 23 of the Dvara Bill, 2018

Section 23. Powers and Functions of the Data Protection Authority

…(4) Supervision and enforcement:…

(d) Any enforcement action authorised by the Data Protection Authority must be proportionate to the contravention of the provision of this Act, or any order or direction issued by the Data Protection Authority under this Act, in respect of which such an enforcement action is authorized;

(e)The Data Protection Authority must consider the following factors while determining the enforcement action to be taken against an entity:

i. the nature and seriousness of the contravention of the provisions of this Act, or any order or direction issued by the Data Protection Authority under this Act, by the entity,

ii. the consequences and impact of the contravention of the provisions of this Act, or any order or direction issued by the Data Protection Authority under this Act, including the extent of,

(1) benefit or unfair advantage gained by the entity as a result of the contravention; and

(2) loss and harm caused, or likely to be caused, to individuals as a result of the contravention;

(3) repetitive or continuing nature of the contravention default prior to the enforcement actions; and

(4) other contraventions committed by the entity under this Act.

2.2.2. The DPA must periodically publish results of inspections and complaints

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.

This is a serious omission that will reduce the transparency and accountability of the DPA. Especially given the powerful enforcement tools at the disposal of the DPA and its wide discretion in deploying them, it is imperative that the DPA is subject to strong disclosure and reporting requirements to ensure it is exercising its powers in a legitimate manner.

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 the context of the Bill, publishing results of inspections and investigations can benefit all stakeholders and improve effectiveness of the new law, as doing so 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, we recommend:

- the re-instatement of requirements in the Bill to publish reports setting out the results of inspections or inquiries in the public interest (as at section 60(2)(w) in the previous Bill);
- the addition of reporting obligations for the DPA as a new function in section 60, mandating that the DPA release **monthly** reports on complaints received and **annual** reports on enforcement actions and complaints acted upon (together with qualitative commentary). Box 2 below suggests some relevant language that may be included to enable such reporting.

Box 2: DPA's Reporting Requirements
Extract from section 23 of the Dvara Bill, 2018

Section 23. Powers and Functions of the Data Protection Authority

…(10) **Reporting:** The Data Protection Authority shall release a report providing aggregate details:

(a) every month, on the complaints received including the number, nature, category, geography, sector and such other factors relating to the complaint as appropriate; and
(b) annually, on the enforcement actions undertaken and complaints acted upon using a format stipulated by the Authority, including such qualitative commentary as it sees fit.

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 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 G. , 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. Fair and reasonable processing should be an overarching obligation on data fiduciaries and data processors.

The Bill requires every person processing personal data to do so in a fair and reasonable manner (section 5(a)). However, unlike in the previous Bill where this obligation was provided in an independent provision, the obligation is mentioned in the Bill as a sub-clause under section 5 (*Limitation on purpose of processing of personal data*). This change in the position of the provision could create an impression that the fair and reasonable obligation is not an overarching obligation while processing personal data, but that it is limited when specifying the purpose of processing. In addition, the obligation would no longer appear to apply when entities claim exemptions from obligations under Chapter VIII of the Bill. Under the previous Bill, the obligation to undertake fair and reasonable processing was an overarching obligation that applied to all stages of data processing activities. This was a creditable inclusion that protected users, especially as no derogations from this obligation were allowed, even when data

fiduciaries received exemptions from other obligations in the Bill (i.e. by claiming exemptions for national security purposes, journalistic purpose or research purposes etc. under Chapter IX of the previous Bill) (Dvara Research, 2018b). Violations of this obligation under the previous Bill could attract penalties up to Rs. 15 crores or 4% of their worldwide turnover.

We had welcomed the addition of this obligation as a standard that could protect data principals even in cases where all their other rights are vacated under other exemptions or grounds for processing (Dvara Research, 2018b). We noted that the criteria for "*fair and reasonable processing"* obligations could be developed drawing from Indian jurisprudence around reasonableness and proportionality in data protection, as well as the experience of data regulators in other jurisdictions like the EU GDPR (EU Regulation 2016/679, 2016), the guidelines issued by the UK ICO (Information Commissioner's Office, 2018), the Kenyan Data Protection Bill, 2018 (The Data Protection Bill of Kenya, 2018) and the Federal Trade Commission Act 1914 (Federal Trade Commission Act, 2010).

Unfortunately, there is a risk that such an overarching obligation no longer exists in the current Bill. Specifically, there is no longer an overarching obligation for fair and reasonable processing for Government when it accesses personal data under the State use exemption in section 35 of the Bill. Section 36 exempts the Government from all obligations for data fiduciaries except purpose limitation obligations in section 4 (*Prohibition of processing of personal data)* and data security requirements section 24 (*Security safeguards)*. The change in the position of the "fair and reasonable processing" obligation from section 4 to section 5, therefore could have the effect of no longer requiring the Government to process data fairly and reasonably, even where it has otherwise been exempted from data protection obligations in the Bill.

This drastically reduces the protection available to data principals, who were previously assured basic fairness and reasonableness in how their personal data was processed even if none of the other protections of the Bill applied.

Accordingly, it is recommended that the fair and reasonable obligation in the Bill should be reinstated as an overarching non-derogable obligation for all data fiduciaries to whom the Bill applies. This could be done by including a reference to section 5 in the lead-in language for section 36, as follows:

> "*The provisions of Chapter II except section 4* ***and section 5****, Chapters III to V, Chapter VI except section 24, and Chapter VII shall not apply where…*"

5. "Harm" should not be 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. Further, these adverse outcomes are not explicitly required to arise from the misuse of personal data. It does not offer a clear substantive or

conceptual definition of harm, or a 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). This will create many problems under the rules of statutory interpretation, including the risk that it excludes future, unforeseen data harms that are currently not contemplated by the list (Dvara Research, 2018b).

Despite this, twenty-three significant provisions in the Bill are contingent on the occurrence of "harm" of which–

- 3 provisions relate to the exercise of their rights by data principals and access grievance redress forums[3], placing a burden on them to prove "harm" has taken place;
- 9 provisions relate to the fulfillment of data protection obligations by data fiduciaries[4], for e.g. requiring them to assess whether "harm" has taken place before fulfilling certain obligations and
- 11 provisions relate to the enforcement of the Bill by the Central Government and the DPA, requiring an assessment of harm by the authorities.[5]

This treatment of harm in the Bill can compromise consumer protection, business certainty and effective regulation. It is highly problematic to have rights and obligations predicated upon proving the existence of harm, especially since the definition suffers from the shortcomings noted above. Accordingly, it is submitted that "harm" should not be a condition on which rights and obligations depend in the Bill. These rights and obligations should be fulfilled irrespective of the occurrence of harm.

Instead, we submit the following approach should be taken (as we have previously highlighted) (Dvara Research, 2018b):

- avoid using "harm" as a threshold or trigger for any substantive obligations or entitlements under the draft Bill. Instead, a broad "right against harm" which imposes a reasonable

[3] *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)).

[4] *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)),

[5] *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)).

obligation on data fiduciaries to avoid causing harm would be a good starting point to protect users and incentivise better data practice, without the confusion and potential impunity that might arise from the current formulation;

- to protect users from harm not contemplated by the obligations and rights currently included Bill, a broader definition of "harm" could be incorporated along with reasonable efforts obligations for fiduciaries to avoid causing harm. This approach would allow future jurisprudence and data practice to develop around this currently inchoate term. 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."

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, Implementing the Personal Data Protection Bill: Mapping Points of Action for Central Government and the future Data Protection Authority in India, 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.

SECTION II: CHAPTER-WISE ANALYSIS

In this section, we present a Chapter-wise analysis of the Bill along with recommendations. Analysis on each Chapter of the Bill is presented in two parts.

- Part A provides a comparative analysis of changes in provisions of the Bill compared to the previous Bill. This is presented in a table format where the first column (titled "Provision (2018)") summarises the substance of provisions of the previous Bill, the second column (titled "Provision (2019)") indicates the corresponding provision in the 2019 Bill and the third column presents analysis on the impact of the change.
- Part B highlights persisting issues in the text of the Bill (from the previous Bill) that remain to be addressed for a more robust data protection regime. This is included where relevant for each Chapter of the Bill.

The comparisons with the previous Bill aim to capture significant changes that have a clear positive or negative impact in the Bill. Very minor changes of words, merged clauses, deletions etc. have not been included unless they have an impact on the substance of the Bill. Recommendations are also included to improve the Bill from a consumer protection perspective, where we have a considered view on these matters.

Chapter I: Preliminary

A. Comparative analysis of changes in the Bill

Provision (2018)	Provision (2019)	Description
s.1(3) (Commencement) Specific timeframes for implementing all the provisions of this Bill were prescribed.	s.1(2)	**Provision**: The provision no longer prescribes specific timeframes within which all the provisions in the Bill must be implemented. The absence of transitional provisions in the Bill creates sizeable uncertainty for data processors and data fiduciaries about when all the provisions will come into force. The previous Bill 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 data fiduciaries and data processors, which could be crushing in the absence of a phased transitional period. Further, absence of transitional provisions in the Bill could weaken political will and industry support to implement the Bill. This has a direct adverse impact, undermining the impetus to create an Authority and related machinery to enforce the Bill's provisions.
s.2(3) (Applicability): The provisions of this Bill did not apply to processing of anonymised data.	s.2(B) (read with s.91(1) & (2))	**Provision**: The provisions of the Bill now apply to non-personal data and anonymised data only to the extent that it is required for under section 91. Sections 91(2) and 91(3) of the Bill give selective powers to the Central Government to direct data fiduciaries and data processors to hand over anonymised or non-personal data for use in service delivery and policy-making. The extension of provisions of the Bill to anonymised data is inconsistent with the scheme of the Bill. Non-personal data or anonymised data is 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. 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. It is submitted that the words "*other than the anonymised data referred to in section 91*" should be omitted from section 2(B), and section 91(1) and (2) should be removed from the Bill.

B. Analysis of persisting issues in the Bill

1. Anonymisation as defined in the Bill is impossible to achieve:

Section 3(2) of the Bill defines anonymisation as an "*irreversible*" process by which the data principal can no longer be identified using the personal data in question. Absolute irreversibility is recognised to be unachievable at present (Al-Azizy, Millard, Symeonidis, Keiron, & Shadbolt, 2015). Methods of anonymising data which meet the required standards today may become vulnerable to new techniques of re-identification due to the continuous development of technologies. Instead, it is submitted that a standard of "*identifiability"* should be applied whereby data is considered anonymous where it can no longer directly or indirectly identify a natural person. This is also in line with the definition of personal data which section 3(28) of the Bill defines as any data "*about or relating to a natural person who is directly or indirectly identifiable*".

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

As set out in detail on page 18, the definition of *harm* in the Bill is highly problematic. Rights and obligations should not be made conditional on this definition given its shortcomings. Detailed reasons for this view are presented in Section I (Overarching Comments), Item 5 at page 18 above. Instead, we submit the following approach should be taken (as we have previously highlighted) (Dvara Research, 2018b):

- avoid using "harm" as a threshold or trigger for any substantive obligations or entitlements under the draft Bill. Instead, a broad "right against harm" which imposes a reasonable obligation on data fiduciaries to avoid causing harm would be a good starting point to protect users and incentivise better data practice, without the confusion and potential impunity that might arise from the current formulation.
- To protect users from harm not contemplated by the obligations and rights currently included in the Bill, a broader definition of "harm" could be incorporated along with reasonable efforts obligations for fiduciaries to avoid causing harm. This approach would allow future jurisprudence

and data practice to develop around this currently inchoate term. 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."*

3. The age threshold included to define a child in the Bill should be reconsidered:

Section 3(8) defines a "*child"* as a person who has not completed 18 years of age. Related obligations in Chapter IV (P*ersonal data and sensitive personal data of children*) mandate that a child's age must be verified, and their parent or guardian's consent must be taken prior to processing that child's data. This could severely restrict children's ability to access data-driven services. While digital safeguards for child protection should be encouraged, it is submitted that, especially for older children, the age threshold and related obligations should be reconsidered and be more nuanced or graded. There is precedent for this in Indian law. For e.g. the Reserve Bank of India allows minors between the age of 10 and 18 to operate bank accounts independent of their parent or guardian (Reserve Bank of India, 2014). In the European Union's General Data Protection Regulations (henceforth "EU GDPR"), the age of lawful consent at 16, allowing members states to reduce it to the age of 13 (EU Regulation 2016/679, 2016). Australia allows entities to presume that children over 15 have "*the capacity to consent, unless there is something to suggest otherwise*" (Office of the Australian Information Commissioner, 2018).

Chapter II: Obligations of Data Fiduciaries

A. Comparative analysis of changes in the Bill

Provision (2018)	Provision (2019)	Description
s.4 (Fair and reasonable processing): Any person who processed personal data owed a duty to the data principal to process personal data in a fair and reasonable manner.	s.5(a)	**Provision**: Every person processing personal data should do so in a fair and reasonable manner. The previous Bill included the obligation to process personal data in a fair and reasonable manner as an independent provision. The 2019 Bill includes it as a sub-clause under section 5 (*Limitation on purpose of processing of personal data*). Our concerns with this change have been set out in detail in Section I (Overarching Comments), Item 4 at page 17 above. There is a risk that this an overarching obligation to process personal data in a fair and reasonable manner no longer exists in the current Bill. where exemptions are claimed under Chapter VIII. Specifically, there is no longer an overarching obligation for fair and reasonable processing for Government when it accesses personal using the State use exemption in section 35 of the Bill. Section 36 exempts the Government from all obligations for data fiduciaries except purpose limitation obligations in section 4 (*Prohibition of processing of personal data)* and data security requirements section 24 (*Security safeguards)*. This drastically reduces the protection available to data principals, who were previously assured basic fairness and reasonableness in how their personal data was processed even if none of the other protections of the Bill applied. Accordingly, it is recommended that the fair and reasonable obligation in the Bill should be reinstated as an overarching non-derogable obligation for all data fiduciaries to whom the Bill applies.

s.8(3) (Notice): An exception to the obligation to provide notice to data principals when processing data for **prompt action** purposes, if doing so would the notice would substantially prejudice the purpose of processing.	s.7(3)	**Provision**: The exceptions to the obligation to provide notice to data principals when processing their personal data non-consensually has been substantially widened. As per section 7(3) (*Requirement of notice for collection or processing of personal data),* providers need not give notice to individuals whose personal data they are processing where it would "*substantially prejudice"* the purpose of processing on *any* of the non-consensual grounds allowed in the Bill. For the reasons set out in detail in item 1.1 of Section I (Overarching Comments) at page 4, this new exception to the rule to provide notice to users should not be included in the Bill. The wide exceptions could adversely affect users' ability to assess how their data is being used and identify contraventions in the processing of their data. It 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 (Dvara Research, 2020). It is submitted that the waiver of obligations to provide users notice of use of their data, should only be allowed in cases of severe emergency (as was the case in the previous version of the Bill).
s.11(2) (Accountability): Data fiduciaries must demonstrate that processing activities comply with provisions of the Bill.	No comparable provision	**Provision**: The obligation of accountability included in the previous Bill does not exist in the new Bill. Under that obligation, data fiduciaries should be able to demonstrate that any processing it undertakes is in accordance with the provisions of this Act. Reinstating this provision will hold data fiduciaries to a higher standard of accountability.

B. Analysis of persisting issues in the Bill

1. Purpose Limitation obligations are weakened by allowing personal data processing for "incidental or connected to" purposes:

Sections 5(a) and (b) of the Bill set out purpose limitations for data processing by only allowing data fiduciaries to process data for specified purposes. We welcome the inclusion of these obligations. However, section 5(b) also allows personal data to be processed for purposes "***incidental or connected with such purpose***". This greatly expands the scope of the clause and waters down the purpose limitation protections afforded in the provision. It is submitted that purpose limitation in Indian law should not be watered down by the use of this language.

Accordingly, section 5 should require that personal data must only be used for specified purposes for which it is collected and not be further processed in any way incompatible with those purposes.

2. Notice requirements should ensure accessibility to data principals with different literacy levels and language preferences:

Section 7(2) of the Bill mandates the notice to be *"clear, concise and easily comprehensible to a reasonable person and in multiple languages where necessary and practicable"*.

This is appreciated and welcomed; however, this clause would benefit from incorporating well-recognised principles that help make notices more meaningful (Dvara Research, 2018b). It is submitted that the notice should be accessible to every data principal in a form that is most appropriate for their literacy levels and language preferences. Data fiduciaries should be encouraged to actively design measures that make the notice conspicuous, intelligible and relevant for the data principal.

The following language could be used in Section 7 to ensure that notices are:

> *"conspicuous, concise, timely, updated, transparent, intelligible and easily accessible form written in clear, plain and understandable language both in English and predominant language of the individual's geographical area and, where a significant portion of the population has limited literacy skills, in a visual and written format, in a form that can be retained and provided free of cost to the individual."*

This language was also submitted in response to public consultation on the White Paper of the Committee Experts, to give effect to the recommendations above (see section 15(1) of the Dvara Bill) (Dvara Research, 2018a).

Chapter III: Grounds for processing of personal data without consent

A. Comparative analysis of changes in the Bill

Provision (2018)	Provision (2019)	Description
s.17(1) (Processing for reasonable purposes): Personal data of a data principal may be processed if it is considered necessary for specified reasonable purposes.	s.14(1)	**Provision:** This provision allows data fiduciaries to undertake non-consensual processing of personal data when necessary for "reasonable purposes". Such "reasonable purposes" will be specified by the DPA through regulations and certain purposes are already included in the text of the Bill. Data fiduciary can process personal data pursuant to this ground under section 14(1), will be required to take "***into consideration***– *a. the interest of the data fiduciary in processing for that purpose;* *b. whether the data fiduciary can reasonably be expected to obtain the consent of the data principal;* *c. any public interest in processing for that purpose;* *d. the effect of processing activity on the rights of the data principal; and* e. *the reasonable expectations of the data principal having regard to the context of the processing.*" (emphasis added) Currently, the data fiduciary is only required to consider these factors when using data under this ground. Instead, it is submitted that the data fiduciary must mandatorily **balance these factors** before specifying reasonable purposes. This means that the data fiduciary must determine whether its interests in processing personal data on this ground outweigh the interests of the data principal. The provision should prohibit data fiduciaries from processing personal data on this ground if data fiduciaries' interests outweigh the interests of the data principals. Such a requirement to balance interests is well recognised in data protection regulation globally. Regulations in other jurisdictions require similar assessments which consider the impact of processing activities on the rights and interests of data principals (Information Commissioner's Office, n.d.); (Article 29 Data Protection Working Party, 2014)

s.17(2) (Processing for reasonable purposes): The DPA may specify reasonable purposes for which personal data may be processed.	s.14(2)	**Provision:** Section 14(2) provides an illustrative list of purposes which can be specified as a "reasonable purpose" by the DPA. It states that the "*"reasonable purposes" may include–* *a. prevention and detection of any unlawful activity including fraud;* *b. whistle blowing;* *c. mergers and acquisitions;* *d. network and information security;* *e. credit scoring;* *f. recovery of debt;* *g. processing of publicly available personal data; and* *h. the operation of search engines.*" No clear criteria appear to guide the selection of the nine activities that can be specified as "reasonable purpose". This appears to be a random or arbitrary list of activities. The lack of connection of the activities noted in the clause itself creates an impression of an arbitrary list, elements of which do not share any common features. This could create problems at two levels and set back the future use of this clause by a DPA. First, in its current form, the clause fails to provide legislative guidance to a future DPA as to the categories of activities that may be specified as "reasonable purposes" in the future. The clear criteria guiding the selection of items in section 14(2) must be stated in the Bill. Statutory drafting principles require that when a general word is followed by a list of specific items or words, they guide the future construction of that general word. This rule -- commonly known as *ejusdem generis* -- simply translates to "*of the same kind*" in Latin. It is used when a statute includes a list of items and indicates that other items "*of the same kind"* as those in the list may also be included to expand the list in the future. The rule helps in identifying the common thread in all listed items, and decide whether an unlisted item can be counted as being in the same class of items or not(Singh G. , 2019). . Second, if no such criteria exist at all there is a risk that this clause and this list can be seen to be an arbitrary selection (and clause) overall. Accordingly, section 14(2) must prescribe clear criteria that the DPA can refer while specifying reasonable purposes and ensure that the items listed fulfil these criteria.

s.17(3)(b) (Processing for reasonable purposes): The DPA determines which activities under "reasonable purposes" will attract the requirement to issue Notice to data principals.	s.14(3)(b)	**Provision:** While releasing regulations specifying "reasonable purpose" under section 14, the DPA can specify if the obligation to provide "*notice under section 7 shall apply or not apply*" to data fiduciaries that process personal data for reasonable purposes. For the reasons set out in detail in item 1.1 of Section I (Overarching Comments) at page 4, this new exception to the rule to provide notice to users should not be included in the Bill. This could adversely affect users' ability to assess how their data is being used and identifying contraventions in the processing of their data. It 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 (Dvara Research, 2020). It is submitted that the waiver of obligations to provide users notice of use of their data, should only be allowed in cases of severe emergency (as was the case in the previous version of the Bill).
s.22(1) (Further categories of sensitive personal data): The DPA had the power to notify categories of personal data as "sensitive personal data"	s.15(1)	**Provision**: The Central Government has the power to notify categories of personal data as "sensitive personal data" in consultation with the DPA and sectoral regulators. The DPA had this power under the previous Bill. The 2019 Bill has shifted this power to the Central Government from the DPA, although still requiring consultation with the DPA and relevant sectoral regulators. It is advisable for the DPA to retain this power as was the case in the previous Bill, as it will have a day-to-day understanding of data practices because of its proximity to the market and its regulatory peers, compared to the Central Government.

B. Analysis of persisting issues in the Bill

1. Stricter criteria for grounds for processing of personal data by an employer should be maintained to prevent abuse of power:

Section 13 (*Processing of personal data necessary for purposes related to employment etc.)* provides an employer (as the data fiduciary) access to the personal data of an employee (data principal). The language in section 13(2) is of grave concern as it allows for employers to process employee data **without consent** if the employer makes a determination that it is "*not appropriate*" or involves "*disproportionate effort*" to request consent from an employee or a potential employee.

This introduces a unilateral and subjective assessment for employers which could be abused and consequently place employees in vulnerable situations. Employers, as data fiduciaries are privy to the personal data of individuals at various points; and it is acknowledged that employers have to collect and process personal data for carrying out their functions and it may be unreasonable for an employer to obtain valid consent from such data principals each time their personal data may be used.

It is suggested that:

- consent should generally be taken by employers before accessing employee data;
- where employers cannot take consent of employees, section 13 must:
    - require the DPA to issue regulations with objective criteria to guide and fetter the discretion of employers, and;
    - file a justification when accessing such data in writing with their Data Protection Officer or the DPA.

Chapter IV: Personal data and sensitive personal data of children

A. Comparative analysis of changes in the Bill

Provision (2018)	Provision (2019)	Description
s.23(3)(d) (Processing of personal data and sensitive personal data of children): The DPA could specify other factors that must be considered for specifying manner of verifying children's age.	s.16(3)(d)	**Provision**: The Central Government has the power to prescribe other factors that must be considered for specifying manner of verifying children's age. This power rested with the DPA in previous Bill, rather than the Central Government as in this 2019 Bill. This power should be retained with the DPA since it also has the primary rule making power in this case. The DPA will also have more proximity to the market and its regulatory peers, making it better equipped to determine such factors.

Chapter V: Rights of data principals

A. Comparative analysis of changes in the Bill

Provision (2018)	Provision (2019)	Description
No comparable provision	s.17(3) (Right to confirmation and access): Data principals have the right to access details about their personal data shared with other entities in one place	**Provision**: Data principals have a right to access the identities of all data fiduciaries with whom their personal data has been shared along with details about the categories of personal data that have been shared. This addition is appreciated as it provides visibility to data principals on how their personal data is being used.
No comparable provision	s.18(1)(d) (Right to correction and erasure) Data principals have the right to erasure of their personal data that is no longer necessary for processing.	**Provision**: Data principals have the right to erasure of their personal data. When personal data is no longer necessary for the purpose for which it was processed, data fiduciaries are now required to delete it. The addition of this right is welcomed.
No comparable provision	s.20(5) (Right to be forgotten): Persons aggrieved by a decision under this	**Provision**: Any person aggrieved by an order by an Adjudicating Officer with respect to their application to exercise their right to be forgotten can appeal to the Appellate Tribunal This provision was absent in the previous Bill. It is a welcome development as it provides additional recourse to a person in exercising their right to be forgotten.

	provision can appeal to the Appellate Tribunal	
s.28(6) (General conditions for the exercise of rights): Rights of data principals had to be exercised in a manner that may be provided by the law, or in a reasonable format that had to be followed by each data fiduciary in the absence of such a law.	No comparable provision	**Provision**: Previously, the format for the form by which rights could be exercised was also to be specified by law or otherwise a reasonable format. This is no longer a requirement in the Bill. Retaining such a requirement in the Bill could enable the development of a clearer procedure and basic minimum standards to be followed by data fiduciaries when processing data principals' requests for exercising rights. A parallel is found in the standardisation of forms under the RTI Act, for instance has made it simpler for the request of data and also forced some level of accountability by mandating certain responses (Government of India, 2005)

B. Analysis of persisting issues in the Bill

1. Loopholes to the right to data portability should be addressed:

We welcome the inclusion of the right to data portability in the Bill. However, some loopholes in the provision should be addressed to ensure the right is not side-stepped by data fiduciaries. Two carve-outs or "loopholes" are set out below.

- The lead-in language in section 19(1) restricts the right to situations where automated means are used to process personal data. "Automated means" is defined in the Bill as "*any equipment capable of operating automatically in response to instructions given for the purpose of processing data*". This could create a gap whereby data analysed by human analysts using programmes and statistical modelling techniques that are not automated would be exempt from the requirement to port data upon request. Accordingly, the language "processing has been carried out through automated means" should be removed from this sub-section.
- Under 19(2)(b), data portability is not required to be complied with by data fiduciaries where it reveals a trade secret or is not "*technically feasible"*. The inclusion of the language on "*technical feasibility*" is vague and imprecise. This could create incentives for data fiduciaries to set up their processing activities in divergent ways to create complexities that do not make it feasible to share data.

2. High barriers to the exercise of data principal rights must be removed:

Section 21 (*General conditions for the exercise of rights*) sets out the procedure to be fulfilled for the exercise of any of the rights in this Chapter. It creates multiple barriers to the exercise of rights which is very troubling. A future law should try to improve rather than restrict the access and use of rights it is trying to vest, if it seeks to give such rights any meaning at all.

(i) ***Rights can be exercised only upon submission of a request in writing or through a consent manager***: In order to exercise a right, a data principal is required to make a written request to a data fiduciary, together with information that satisfies the data fiduciary as to their identity. This automatically creates a very high barrier to entry in our country, where only 21.8% have access to education beyond matriculation / secondary level (Office of the Registrar General & Census Commissioner of India, 2015). Due to lack of clarity on the implementation of a *consent manager*, it is difficult to assess whether it would be a suitable alternative to the requirement of written requests to exercise data principal rights. This requirement should be amended to require data fiduciaries to entertain requests through multiple channels and modes including online lodging, toll-free calling lines, e-mail, letter, fax or in person.

(ii) ***Fee for exercise of rights***: Section 21(2) 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).

(iii) ***No requirement to respond to requests to exercise rights promptly***: Section 21(3) allows the DPA to specify a "*reasonable time period*" within which request from data principals should be complied with. Instead, a clear time period should be stipulated for the data fiduciary to respond to requests. This section should be amended to stipulate that data fiduciaries must comply with requests "*within a reasonable time not to exceed ten business days*" (Dvara Research, 2018a).

(iv) ***Substantial burden on data principal following rejection of rights:*** Section 21(4) creates a disproportionate burden on the data principal seeking to exercise rights to once again lodge a formal complaint with the DPA upon the rejection of such a right. Instead, where the data fiduciary rejects a data principal's request to exercise a right, there must be an automatic referral of this rejection to the internal grievance redressal procedure as envisioned in section 39(3) of the Bill. If there is no satisfactory resolution within 30 days of this referral, the

data principal should be provided full details of how a complaint can be made to the DPA through a variety of modes including online lodging, toll-free calling lines, e-mail, letter, fax or in person.

(v) ***Data fiduciary may reject requests if it could harm of other data principals****:* Section 21(5) enables data fiduciaries to deny requests to exercise rights where such compliance could harm the rights of another data principal. There are no doubt situations where other data principals could be affected by one person's request to access, correction, updating, erasure or porting of information which is inextricably linked with theirs. A blanket power to refuse requests to exercise rights could give data fiduciaries unilateral power to refuse inconvenient requests under the ruse that they may cause other data principals harm. Rather than the blunt method of summarily rejecting requests, data fiduciaries should be required to (a) undertake a balancing test, taking into account the public interest and the effects on other data principals; and (b) seek to give effect to the right of the requesting data principal, by masking or removing the information pertaining to others who may be impacted by this request to the best extent possible.

Chapter VI: Transparency & accountability measures

A. Comparative analysis of changes in the Bill

Provision (2018)	Provision (2019)	Description
s.29 (Privacy by Design): Required all data fiduciaries to *implement* policies and measures to ensure Privacy by Design.	s.22	**Provision:** Section 22 requires data fiduciaries to prepare a Privacy by Design (PbD) policy of data processing for their organisations. Such policies may be submitted for certification to the DPA. The PbD obligation has been weakened in this new articulation. Previously, the obligation was for entities to **implement** PbD in all their practices and technical systems. In the new Bill, the obligation now is to merely **prepare a PbD policy**. The procedure for certification of the PbD policies by the DPA, and their publication on websites of the DPA and data fiduciary are new additions to the provision. In the current form, section 22 could limit the incentive of 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) could be re-instated.
No comparable provision	s. 23(3)-s.23(5) (Consent managers): Data principals can give or withdraw their consent through a consent manager that is registered with the DPA.	**Provision:** These provisions introduce a new data fiduciary, '*consent managers',* in the Bill. Consent managers are defined as data fiduciaries created specifically to enable data principal to gain, withdraw, review and manage their consent through an accessible transparent, interoperable platform. Any action related to consent-withdrawal, giving or reviewing consent by the data principal via a consent manager will be treated at par with direct communication from the data principal. The introduction of consent manager appears to be a technological solution to help data principals communicate their consent or the lack of it to data fiduciaries. It appears to be a dashboard, designed for smartphones, with a view to afford the data principal greater autonomy in how their data is held and used. The efficacy of the consent managers appears to be directly related to (i) users' ability to comprehend the terms and conditions of the use of their personal data and make an informed choice about consenting to a particular data use, (ii) their ability to afford and operate smartphones. Both these assumptions are widely contested both in global research on

		consent, but more importantly given India's unique context. By digitising these consent forms, the users will be exposed to the same lack of choice that they face today. Instead of replicating these deficiencies, consent managers could redesign consent, when digitising it. Our primary study suggested that users' who may not be able to read or write, prefer icons and visual depiction of the most salient terms and conditions (CGAP, Dalberg, Dvara Research, 2017).
No comparable provision	s.26(4) (Social media intermediaries): Social media intermediaries can be notified as significant data fiduciaries depending on their functions and number of users.	**Provision:** This provision in the Bill empowers the Central Government (in consultation with the DPA) to notify a social media intermediary as a significant data fiduciary. While notifying a social media intermediary as a significant data fiduciary two factors will be considered, i.e. (i) the number of users and (ii) the impact of the social media intermediary for electoral democracy, security of state, public order. The explanation to the provision suggests that commercial or business-oriented transactions, provision to access to the internet and search engines, on-line encyclopedias and email services are excluded from the definition of social media intermediary. This provision appears to inconsistent with the scheme of delegation of powers in the Bill which empowers the DPA to determine and notify significant data fiduciaries (in section 26(1)). It is submitted that all determinations regarding significant data fiduciaries (including if social media intermediaries fall in this category) should be retained with the DPA. The DPA could act in consultation with the Central Government were such classification of social media intermediaries is tied to interests of electoral democracy. In addition, well -reasoned parameters and guidelines should be created *ex-ante* to determine the criteria for significant data fiduciaries (including social media intermediaries) to guide such categorization and to ensure they are not arbitrary.
s.35(3) (Civil penalties for data auditors): Empowered the DPA to specify form and manner of data audits and civil penalties for data auditors.	s.29(3)	**Provision:** Previously, the Bill had a provision that enabled the levying of civil penalties by the DPA on data auditors where they were negligent in their audits. The Bill removes this. This could weaken the accountability of data auditors. In the absence of clear sanctions for negligence, there is a potential for a misalignment of incentives for data auditors who will be paid by the entities for whom they conduct audits. It is recommended that the ability for the DPA to levy civil penalties for negligence be re-inserted in section 29(3).

B. Analysis of persisting issues in the Bill

1. 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 mandates a data fiduciary to make a subjective determination of how harmful its data breach is likely to be to data principals. This determination forms the basis to decide if the DPA needs to be notified about 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).

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.

Chapter VII: Restriction on transfer of personal data outside India

A. Comparative analysis of changes in the Bill

Provision (2018)	Provision (2019)	Description
s.40 (Cross border transfer of data): The relevant chapter dealt with transfer of personal data, sensitive personal data and critical personal data out of India.	s.33	**Provision**: The previous Bill referred to three categories of data that could be transferred across borders (i) personal data (ii) sensitive personal data and (iii) critical personal data. This resulted in a lack of clarity regarding these categories and the rules that applied to them (Dvara Research, 2018b). The Bill now contains a simpler framework of two categories of personal data that are subject to restrictions or conditions for transfer (i) sensitive personal data and (ii) critical personal data. It has also introduced more clarity on the treatment of these two categories of data, with respect to transfers to third countries. This is noted as a positive development.

B. Analysis of persisting issues in the Bill

1. There is lack of clarity in the definition of Critical Personal Data:

Section 33(2) states "*critical personal data"* can only be processed in India and cannot flow outside our country's borders. However, the term is not defined and the Explanation to section 33(2) stated that the term will include such personal data as notified by the Central Government. Some criteria need to be provided in the primary legislation to indicate the nature of personal data that could be notified to limit disruptions to the digital economy, which could result from regulatory uncertainty.

Chapter VIII: Exemptions

A. Comparative analysis of changes in the Bill

Provision (2018)	Provision (2019)	Description
s.42: (Security of the State): This provision set out an exemption from large parts of the previous Bill in the interests of security of the State. Despite the exemptions, obligations under section 4 (*fair and reasonable processing*) and section 31 (*security safeguards*) remained.	s.35	**Provision**: This provision empowers the Central Government to exempt any agency of the State from any/all provisions of the Bill by order if it is satisfied that the exemption is necessary or expedient (i) in the interest of sovereignty and integrity of India (ii) security of the State (iii) friendly relations with foreign states (iv) public order (v) preventing incitement to the commission of any cognizable offence relating to the aforementioned. The provision empowers the Central Government to exempt State agencies from the requirements of the data protection law through executive orders, without any specific safeguards prescribed in the text of the Bill itself. Section 35 merely states that the order passed to create the exemption should prescribe any "*procedure, safeguards and oversight mechanism*". This provision significantly expands the grounds on which the exemption for State agencies can be claimed. It removes the conditions that existed in the previous Bill (at section 42) before such an exemption could be claimed, i.e. that it must be brought into effect through a law passed by Parliament, and such law is necessary and proportionate to the interests being achieved. The wide powers delegated and the absence of clear safeguards to guide their use by the Central Government Authorities could open this provision up to challenge as being arbitrary or unconstitutional. The new provision may fall short of the three- part test as laid down in *Justice K.S. Puttaswamy v. Union of India* (2017). It is submitted that the formulation of the State exemption in section 42(1) of the previous Bill should be reinstated and strengthened (including through judicial oversight mechanisms) to deliver meaningful data protection to the citizens of India.

s.43, s.44, s.46 & s.47 (Exemptions): Processing personal data for– a. prevention, detection, investigation & prosecution of crime, b. legal proceedings, c. domestic purposes, and d. journalistic purposes was exempted from all provisions except fair and reasonable processing and security safeguards.	s.36	**Provision:** Section 36 exempts the Government from all obligations for data fiduciaries except purpose limitation obligations in section 4 (*Prohibition of processing of personal data)* and data security requirements section 24 (*Security safeguards)*. For the reasons set out in detail in item 4 of Section I (Overarching Comments) at page 17, this could have the effect of no longer requiring the Government to process data fairly and reasonably, even where it has otherwise been exempted from data protection obligations in the Bill. This drastically reduces the protection available to data principals, who were previously assured basic fairness and reasonableness in how their personal data was processed even if none of the other protections of the Bill applied. Accordingly, it is recommended that the fair and reasonable obligation in the Bill should be reinstated as an overarching non-derogable obligation for all data fiduciaries to whom the Bill applies. This could be done by including a reference to section 5 in the lead-in language for section 36, as follows: "*The provisions of Chapter II except section 4* ***and section 5****, Chapters III to V, Chapter VI except section 24, and Chapter VII shall not apply where…*"
Section 45 (Research, writing or statistical purposes): Exemption for the processing for research purposes except from s.4 (fair and reasonable processing), s.31(security safeguards) and s.33 (data protection impact assessment).	s.38	**Provision:** The exemption for research, archiving and statistical purposes in the Bill allows the DPA to completely exempt entities from all the provisions of the Bill. This is wider than the equivalent exemption in the previous Bill, which still required data security obligations, fair and reasonable processing and the conducting of data protection impact assessments where relevant. This reduces the protection available to data principals, who were previously assured at least basic security and fairness in processing even by entities partaking of the Research Exemption.

Section 48: (Manual processing by small entities): Exemption for small entities	s.39	**Provision**: The provision in the Bill now exempts entities from the legislation on the basis of criteria that are not pegged to a static number. Previously this was on the basis of a predetermined monetary turnover (Rs. 20 lakhs) and number of users (100 data principals in the last 12 months). This is a positive development that is welcomed. The DPA will now need to create regulations that consider (i) turnover of data fiduciary in previous financial year; (ii) purpose of collection of personal data, and (iii) volume of personal data processed by such data fiduciary.
No comparable provision	s.40 (Regulatory sandbox): The DPA can create a sandbox for encouraging innovation in emerging technologies.	**Provision:** The Bill has introduced a sandbox for innovation in artificial intelligence, machine-learning or any other emerging technology in public interest. Two concerns are flagged in relation to this provision. • First, entities in the sandbox are exempted from many of the obligations under Chapter II (*Data Protection Obligations)* such as specifying purpose of data collection, limitations on collection and storage of personal data. This is an uncommon vacation of consumer protections and should be rectified. The provision must ensure data principals' rights are extended rather than curtailed in the sandbox, clear redress mechanisms are specified. Sandbox participants ensure that all obligations towards customers are fulfilled before they exit the sandbox. • Second, the objectives and perimeter of the Sandbox should be clarified to avoid the risk of regulatory arbitrage or over-regulation. For instance, the proposed sandbox under the DPA may overlap with the RBI's fintech sandbox which began operation in November 2019 (Reserve Bank of India, 2019).

Chapter IX: Data Protection Authority of India

A. Comparative analysis of changes in the Bill

Provision (2018)	Provision (2019)	Description
s.49(4) (Establishment of the DPA): The DPA may establish its offices at other places in India with prior approval of the Central Government.	s.41(4)	**Provision:** This provision empowers the DPA to establish offices, in addition to the head office, "*at other places in India*", with the prior approval of the Central Government. We welcome the DPA's ability to establish offices in other places. However, we submit that the requirement for regional and zonal offices should be mandatory in the design of the DPA and included in the primary legislation. A nationwide presence of the DPA will enable it to discharge its duties effectively, considering the complexity and vastness of the country. Moreover, considering that the DPA is entrusted to uphold a newly recognised fundamental right, a regional presence will help generate awareness about the fundamental right to privacy and provide effective means for data principals to exercise it. The regional offices could perform the functions of enforcement and grievance redress at the local level and report into a centralised database maintained by the DPA (Raghavan, Chugh, & Kumar, 2019). This approach could potentially: • **Increase the effectiveness of the data protection regime by offering locally accessible points of grievance redress:** Regional offices offer a direct point of access to data principals, enabling them to register their complaints with greater ease in vernacular languages. This could significantly improve the use of the grievance redress mechanism. International best practices also suggest that local and multiple grievance uptake points are essential for an effective grievance redress mechanism (Raghavan, Chugh, & Kumar, 2019). A well-functioning grievance redress mechanism can in turn instil confidence in users and encourage them to

		approach the system more frequently. For instance, the UK's Financial Ombudsman Service (FOS) has seen a ten-fold increase in complaints registered over the last decade (Task Force on Financial Redress Agency, 2016). Regional offices could therefore simplify the process of grievance redress for the data principals, encourage them to engage with the system frequently and improve the effectiveness of the DPA's operations significantly. Moreover, frequent use of the grievance redress mechanism will also increase awareness about rights of data principals and incentivise data fiduciaries to comply with their obligations. • **Increase the efficiency in the enforcement and quasi-judicial functions of the DPA:** For the proposed DPA to be proactive and responsive, it will be required to conduct on-site supervision. Regional offices could increase the efficiency of on-site supervision (Raghavan, Chugh, & Kumar, 2019) by maintaining and deploying regional teams for the purpose. Similarly, performing the quasi-judicial function at the regional level could save costs for adjudication for parties involved and enable the proposed DPA to respond to case-load. • **Several existing Indian regulators also enforce their mandate through similar regional structures:** The Directorate of Enforcement, the specialised financial investigation agency under the Department of Revenue of the Ministry of Finance, runs regional offices with zonal and sub-zonal offices in smaller cities (Directorate of Enforcement, n.a.). Similarly, the Bombay Stock Exchange also handles grievance redress through over 20 Regional Investor Service Centres (Bombay Stock Exchange, 2018). It is therefore submitted that: • the legislation should empower DPA to establish zonal offices at the outset, for the reasons considered above. The DPA could also be vested with the power to expand to the regional level when the need arises. For an indicative structure please refer to our working paper titled "Effective Enforcement of a Data Protection Law" (Raghavan, Chugh, & Kumar, 2019); and

		• the DPA should be empowered to determine the appropriate location for its regional offices, independent of the Central Government. This will allow the DPA to remain agile and flexible when responding to the demand for its operations. Similar powers exist for the RBI under the Banking Ombudsman Scheme (Reserve Bank of India, 2016). We had also emphasised these concerns in our response to the draft Personal Data Protection Bill, 2018 (Dvara Research, 2018b).
s.50(1) (Composition): The DPA shall consist of a chairperson and not more than six full-time members.	s.42(1)	**Provision:** Under this provision, The staff of the DPA will include a chairperson and "*…not more than six whole-time Members…*", of which one hall have qualification and experience in the law. For the reasons set out in detail in item 2.1.1 of Section I (Overarching Comments) at page 4, this provision could weaken the DPA by enabling under-staffing and precluding the appointment of Independent Members. 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. Further, the provision does not specify the minimum number of Members should be that should be appointed to the DPA. It is noted that the comparable provision in the previous Bill (section 50(1)) merely stated that the DPA should consist of a Chairperson and 6 whole time members, leaving open the possibility to appoint Independent Members. It is submitted the Bill should mandate that the Management Board of the DPA is dominated by Independent Members. This is in line with well-established principles of institutional design (Roy, Shah, Srikrishna, & Sundaresan, 2019). Ideally, there should be a requirement for four of the seven Members of the DPA to be independent Members.

s.50(2) (Composition): The Selection Committee appointing the Chairperson & members comprised the Chief Justice or other Supreme Court Judge, Cabinet Secretary, and an Independent expert.	s.42(2)	**Provision:** The Selection Committee for the DPA is now made up of the Cabinet Secretary, and Secretaries to the Law Ministry and MEITy. The composition of the Selection Committee in the previous Bill reflected the balance and expertise required to create a credible new regulator. The current composition comprising solely of Secretaries to the Central Government, could diminish the independence and ability of the DPA to meet the challenges of regulating a dynamic field like personal data processing (Dvara Research, 2020). Item 2.1.22.1.1 of Section I (Overarching Comments) at page 4 details these concerns further. 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).
s.60(2)(w) (Powers & Functions): The DPA had to prepare and publish reports of inspections and inquiries deemed to be in public interest	No comparable provision	**Provision:** The DPA no longer has to prepare and publish reports of inspections and other comments in public interest. This could limit the transparency in the DPA's functioning. Requiring the DPA to publish such reports, would help (i) keep data principals informed about the performance of data fiduciaries, (ii) data fiduciaries understand the DPA's preferred practices and refine internal procedures (iii) create feedback loops to help the DPA identify problems in the system and in its regulations and rectify them expeditiously (Dvara Research, 2020). It would enable the DPA gain trust and legitimacy overall for its actions. This provision should be reinstated in the current Bill.
s.61(1) (Codes of practice): Codes of practice can be issued by the DPA for promoting good practices and facilitate compliance with	s.50(1)	**Provision:** Under section 50(1), codes of practice will be issued as regulations by the DPA. Together with section 61 (*Penalty for contravention where no separate penalty has been provided*), data fiduciaries and processors can be penalised for not complying with regulations issued under the Bill. Codes of practice are meant to serve as a set of practices that entities can voluntarily subscribe to for simplifying their compliance with the law. They are not meant to be

data protection obligations.		mandatory. Entities can choose to create their own codes of practice as long as the codes comply with the law (European Data Protection Board, 2019) (UK Information Commissioner's Office, n.d.) (Office of Consumer Affairs, Canada, 2010). Codes of practice, therefore, are not meant to be mandatory. Regulations, on the other hand, are binding under the law as per Article 13(3) of the Constitution of India, 1950 (Singh M. P., 2003). It is therefore concerning that the Bill requires codes of practice to be issued as regulations, and that data fiduciaries and data processors can be penalised for not complying with them. Compliance with certified codes of practice should not be mandatory in the Bill. The Bill should allow entities to develop their own codes of practice as long as they adopt equivalent or better standards compared to the codes certified by the DPA. We therefore recommend that section 50(1) of the current Bill be replaced by section 61(1) of the previous Bill. We also recommend that the Bill reinstate section 61(10) of the previous Bill which requires the DPA to maintain a register containing all the codes of practice that are in force, to provide convenient access to stakeholders and promote transparency.
s.61(7) and (8) (Codes of practice): Non-compliance with the codes of conduct by the data fiduciary or processor may be considered when determining whether it is in violation of the provisions of the Act	s.50(1)	**Provision:** Under section 50(1) of the Bill, Codes of Practice will be issued as regulations by the DPA. Together with section 61 (*Penalty for contravention where no separate penalty has been provided*), data fiduciaries and processors can be penalised for not complying with regulations issued under the Bill. This is a matter of concern as this provision could penalise data fiduciaries and processors who follow different but equivalent or better codes of practice. Instead, section 61(8) from the previous Bill can be reinstated that allows data fiduciaries and data processors to demonstrate before the DPA, court, tribunal or statutory body that it has adopted an equivalent or higher standard of practices with respect to the codes of practice stipulated.
s.61(10) (Codes of Practice):	No comparable provision	**Provision:** The DPA previously had to maintain a register containing all codes of practice which are in force. The Bill does not include this provision any longer.

The DPA has to maintain a register containing all codes of practice in force which must be public and accessible through its website.		It should be re-instated in the Bill, as the DPA plays an important role in providing information consistently to the broader market on the Codes in place for personal data processing in different sectors.
s.64 (Power to conduct inquiry): The DPA may conduct an inquiry where it has reasonable grounds to believe that the activities of a data fiduciary are detrimental to the interest of the data principals or where a data principal or a data processor has violated any provisions of the Act, prescribed rules, specified regulations or issued directions.	s.53	**Provision:** The DPA is empowered to conduct enquiries on data fiduciaries and data processors whose processing activities are either (i) detrimental to the interests of data principals, or (ii) in contravention with any provisions of this Bill or rules and regulations made by the DPA. The DPA may do so on its own, or on grounds of a complaint received by it. This is a welcome addition to the regulatory powers of the DPA.
s.65 (Action by DPA post-inquiry): After receiving a report from an Inquiry Officer, the DPA may undertake a range of enforcement actions after giving the appropriate data fiduciary or data processor the	s.54	**Provision:** Under this section 53, the DPA is vested with the power to undertake enforcement actions upon the receipt of a report regarding activities of a data fiduciary or a data processor that are (i) detrimental to the interests of data principals, or (ii) in contravention with any provisions of this Bill or rules and regulations made by the DPA under section 53(1) of the Bill. These enforcement actions vary in their punitive effects. The DPA has a wide range of enforcement tools. However, no provisions exist to fetter its discretion for the accountable exercise of these enforcement powers. As set out in great detail in item 2.2.1 of Section I (Overarching Comments) on page 12, the Bill must include discretion-fettering provisions to fetter the discretion of the

opportunity to represent themselves.		DPA to guide it's the extensive enforcement powers of the DPA. Section 54 of the Bill should be modified to include the paradigm of responsive regulation, which has also been alluded to in the Report of the Committee of Experts on Data Protection under the chairmanship of Justice B. N. Srikrishna. This requires that enforcement actions undertaken by a regulator should be proportionate and sensitive to the nature of the contravention. Any enforcement action authorised by the DPA must to be proportionate to the relevant contravention in respect of which the enforcement action is being authorised. Specific factors to drive should determine the choice of enforcement tool by the DPA, such as the nature and seriousness of the contravention, the consequences and impact of the contravention e.g. it including the unfair advantage gained, loss or harm caused, repetitive nature of the contravention etc. and other contraventions committed by the entity. Detailed drafting guidance for how this can be done is available at Box 1 on page 13 above.
s.66(1) (Search & Seizure): The Central Government could authorise a Gazetted Officer to seize documents in a set of circumstances.	s.55(1)	**Provision:** The Inquiry Officer appointed by the DPA can seize documents and records on only a single ground in the Bill, compared to three grounds previously. They can seize documents when records are likely to be tampered, altered, mutilated, manufactured, falsified or destroyed. For any further documents and materials, the Inquiry Officer needs to obtain an order from a designated court. This is a positive development. Judicial oversight over search and seizure powers helps in checking non-arbitrary exercise of power by the DPA.
s.66(8) (Search & Seizure): A person whose documents or records have been seized can appeal to the Appellate Tribunal.	No comparable provision	**Provision:** The previous Bill allowed individuals to approach the Appellate Tribunal to challenge orders for seizure of documents. The Bill does not provide for such recourse. This should be re-instated.

Chapter X: Penalties

A. Comparative analysis of changes in the Bill

Provision (2018)	Provision (2019)	Description
s.74(1) (Levying Penalty): The Adjudicating Officer can levy a penalty only after conducting an inquiry	s.63(1)	**Provision:** In the Bill, the Adjudicating Officer cannot conduct an inquiry to levy a penalty unless the complaint is made by the DPA. This means an individual must compulsorily approach the DPA to register a complaint, which will then be sent on the Adjudicating Officer. This has an impact on an individuals' right to recourse since in cases where the DPA decides not to initiate an inquiry pursuant to the complaint, there is no right to appeal against this decision (Dvara Research, 2020). The provision should be modified to enable a right of appeal to the DPA's determination to the Adjudicating Officer.
s.77(2) (Data Protection Fund): Sums realised by the DPA through penalties will be earmarked for constituting a Data Protection Awareness Fund.	s.66(2)	**Provision**: All sums realised by the DPA through penalties will be credited to the Consolidated Fund of India. We welcome the change in this provision in the Bill. This rectifies the problem in the previous version of the Bill where sums realised from penalties were credited to a separate Data Protection Awareness Fund in the DPA. This deviated from usual practice where all receipts of a regulator are credited to the Consolidated Fund of India.

Chapter XI: Appellate Tribunal

A. Comparative analysis of changes in the Bill

Provision (2018)	Provision (2019)	Description
s.80(1) (Qualifications for Appellate Tribunal members): The Central Government must prescribe qualifications for persons appointed to be Chairperson or member of the Appellate Tribunal	s.68(1)	**Provision:** Previously, the Central Government could prescribe the qualifications for Members of the Appellate Tribunal. Now, the Bill specifies the qualifications for Chairperson and Members of the Appellate Tribunal in its text. It requires that persons should be: - in the case of the Chairperson, a Judge of the Supreme Court or a Chief Justice of a High Court; - for Members, a former Secretary to the Government of India (or any equivalent post) who has served in the position for at least 2 years, or any person well-versed in data protection, information technology etc. This is welcomed as a positive development.
s.80(2) (Terms and conditions): The salary, allowance or any other terms and conditions of the service of the chairperson or any other member of the Appellate Tribunal may be varied to their disadvantage after their appointment.	s.70	**Provision:** Section 80(2) of the previous Bill stated that the terms and conditions of the service of the chairperson or members of the Appellate Tribunal "*may be varied to her disadvantage after her appointment*". This is absent in the Bill. This explicit stipulation provided in the previous Bill was welcome as it ensures independence of the actions of the chairperson and members of the Appellate Tribunal. This provision should be re-instated in the Bill.

Chapter XII: Finance, accounts & audit

A. Comparative analysis of changes in the Bill

Provision (2018)	Provision (2019)	Description
No comparable provision	s.81(4) (Annual summary report prepared by the DPA): The DPA must publish a report of its activities annually.	**Provision:** The Bill now requires annual reports providing a summary of the DPA's activities to be made available to the public. This is a welcome development in the Bill as it increases transparency in the functioning of the DPA.

B. Analysis of persisting issues in the Bill

1. Expense heads of the grants from Central Government to the DPA must be clearly stated:

Section 78 (*Grants by Central Government*) of the Bill requires the Central Government to grant appropriate monetary dispensation as it deems fit to the DPA, for the purposes of the Act. This provision should include language in its text to ensure that the dispensation by the Central Government is compulsory and sufficient for the DPA to discharge its various functions. Other existing legislations include such language to ensure that sufficient grants are secured for the independence of the relevant regulator.

- Section 21 of the Telecom Regulatory Authority of India Act, 1997 requires the Central government after due appropriation made by the Parliament, to

  "*make to the Authority grants of such sums and money as are required to pay salaries and allowances payable to the Chairperson and the members and the administrative expenses including salaries, allowances, and pension payable to or in respect of officers of other employees of the Authority.*"

  This provision sets out the expense heads that should be covered by the Central Government's grant, providing an indication of the quantum of the grant to be made.
- Similarly, Section 13 of the Right to Information Act 2005, requires the Central Government to provide the

"*the Chief Information Commissioner and the information Commissioners with such officers and employees as may be necessary for the efficient performance of their functions under this Act, and the salaries and allowances payable to and the terms and conditions of service of the officers and other employees appointed for the purpose of this Act shall be such as may be prescribed.*"

This provision ensures that the office of the Chief Information Commissioner is equipped with sufficient capacity to discharge their functions.

Similar language should be included in section 78 to specify the expense heads that should be covered by the grant of the Central Government, such as administrative expenses and the cost of personnel deployed by the DPA.

2. The DPA should also report annually on complaints & enforcement actions:

Section 81 (*Furnishing of returns, etc., to Central Government)* of the Bill sets out the reports that the DPA should present to the Central Government. Under this section, the DPA will furnish (i) such returns and statements required by Central Government and (ii) an annual report giving a summary of its activities during the previous year.

In the annual report submitted to the Central Government, while summarising its activities of the previous year the DPA should separately set out a detailed summary of complaints acted upon and enforcement actions undertaken in the year.

The format for this report on complaints & enforcement actions must be consistent across years, including such qualitative commentary as it sees fit to enable a cross multi-year analysis of the DPA's functioning and effectiveness. Such a scrutiny is an important mechanism to hold the DPA accountable for the exercise of the powers vested in it.

Chapter XIII: Offences

A. Comparative analysis of changes in the Bill

Provision (2018)	Provision (2019)	Description
No comparable provision	s.83(2) (Cognizance of offence) Courts shall not take cognizance of offences except on complaints from DPA.	**Provision:** This section provides that a court cannot take cognizance of an offence in the Bill unless the complaint is made by the DPA. It does not allow a person to directly initiate criminal proceedings even if an offence has been committed under the Bill. The person will have no recourse if the DPA does not initiate an inquiry pursuant to the complaint, especially because there is no right to appeal against the DPA's decision in this matter (Dvara Research, 2020). This provision violates the right to seek remedy when there is a violation of law by directly approaching judicial institutions. The Supreme Court had struck down similar provisions in the Aadhaar Act, 2016 on the ground of being arbitrary (*Justice K.S. Puttaswamy (Retd) & Anr v. Union of India & Ors*, 2018). Accordingly, it is submitted that this provision should be removed.
s.94 (Investigating Offences): Only an officer who holds the rank of an inspector or a higher rank can conduct investigations into offences.	No comparable provision	The Bill no longer specifies the officer who can initiate investigations of criminal offences created by this legislation. Laws conferring investigation powers on an officer generally provide qualifications for officers who can conduct investigations. For e.g. section78 of the Information Technology Act, 2000 states that "*a police officer not below the rank of Inspector*" can investigate any offence under the Act. Such provisions specify who is legally enabled to exercise the powers. Since the Bill creates offences, it must specify the officer legally enabled to exercise powers to commence investigations in this regard.

s.98 (Power of Central Government to issue directions): Central Government can issue directions that are binding upon the DPA.	s.86	**Provision**: The Central Government can issue binding directions to the DPA. The Central Government can give the DPA an opportunity to express its views before passing an order if it is practicable. As described in detail at item 2.1.3 of Section I (Overarching Comments) on page 10, this provision further erodes the independence of the DPA and exposes it to the potential for undue governmental interference. An important dimension of regulator's independence is their independence from politics, i.e. independence from governments, parliaments, parties and individual politicians (Koop & Hanretty, 2017) (Hanretty & Koop, 2012). Further, a significant indicator of political independence of regulatory agencies is the degree of independence conferred in them, by the legal instruments that create and govern these agencies (Hanretty & Koop, 2012). To fulfil the vision for a truly independent DPA, it is important to ensure that the DPA's functional independence is not overridden by the directions and diktats of the Central Government.

Chapter XIV: Miscellaneous

A. Comparative analysis of changes in the Bill

Provision (2018)	Provision (2019)	Description
S. 105 (Applicability): No application to non- personal data.	S. 91: (*Act to promote framing of policies for digital economy etc.)*	**Provision**: Sections 91(2) and 91(3) of the Bill give selective powers to the Central Government to direct data fiduciaries and data processors to hand over anonymised or non-personal data for use in service delivery and policy-making. For the reasons set out in the comments to section 2(3) in Chapter I of the Bill (above), it is submitted that this Bill should not contain provisions relating to the processing or sharing of anonymised or non-personal data. The words "*other than the anonymised data referred to in section 91*" should be omitted from section 2(B), and section 91(1) and (2) should be removed from the Bill.
S.108(2)(g) (Power to make regulations): The DPA may make regulations regarding additional factors for determining appropriate age verification mechanisms for processing the personal data of children.	Section 93 (2)(b) (Rules for age verification)	**Provision:** In the Bill, the Central Government is empowered to make specific rules regarding factors to be taken into consideration for the age verification of child. This power was conferred to the DPA in the previous Bill. It is submitted that, the DPA might be in a better position to assess the other relevant factors, as it will have a day-to-day understanding of data practices because of its proximity to the market and its regulatory peers, compared to the Central Government.
S. 107 (2)(y) (Power to make rules): Power to specify the manner of hearing complaints and limit on the amount of compensation.	S. 64(8) & 93(2)(p)	**Provision**: The Bill confers power on the Central Government to prescribe the manner for hearing complaints under compensation. It does not confer power on Central Government to prescribe maximum compensation that can be awarded. Under section 64(4), the Adjudicating Officer will now determine the quantum of compensation. This appears to be a welcome change that allows each case and compensation to be judged on its merits.

References

Article 29 Data Protection Working Party. (2014, April 9). *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.* Retrieved from European Commission: https://www.dataprotection.ro/servlet/ViewDocument?id=1086

Atmospheric Diving Systems Inc. v. International Hard Suits Inc, [1994] BCJ no. 493. (n.d.).

Ayers, I., & Braithwaite, J. (1992). *Responsive Regulation: Transcending the Deregulation Debate.* New York: Oxford University Press.

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

Bombay Stock Exchange. (2018, September 20). *Complaints against Companies and Trading Members.* Retrieved from Bombay Stock Exchange: https://www.bseindia.com/investors/cac_tm.aspx?expandable=2

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

Department of Telecommunications. (n.a.). *LICENSE AGREEMENT FOR UNIFIED LICENSE.* Retrieved from Department of Telecommunications: https://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf

Directorate of Enforcement. (n.a.). *Organisational Chart of the Directorate of Enforcement.* Retrieved from Enforcement Directorate: http://www.enforcementdirectorate.gov.in/offices/organizational_chart.pdf#zoom=150?p1=1188201537437955901

Dvara Research. (2018a). *Data Protection Bill.* Retrieved from Dvara Research: https://www.dvara.com/blog/2018/02/07/our-response-to-the-white-paper-on-a-data-protection-framework-for-india/

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. (2018a, February 7). *The Data Protection Bill, 2018.* Retrieved from Dvara Research: https://www.dvara.com/blog/2018/02/07/our-response-to-the-white-paper-on-a-data-protection-framework-for-india/

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

Dvara Research. (2018b, October 16). *Comments to the Minsitry 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

Dvara Research. (2020). *Initial Comments of Dvara Research dated 16 January 2020 on the Personal Data*. Retrieved from Dvara: https://www.dvara.com/research/wp-content/uploads/2020/01/Initial-Comments-on-the-Personal-Data-Protection-Bill-2019.pdf

Dvara Research. (2020, January 17). *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.* Retrieved from Dvara Research: https://www.dvara.com/research/wp-content/uploads/2020/01/Initial-Comments-on-the-Personal-Data-Protection-Bill-2019.pdf

EU GDPR. (2015). *Art. 45: Transfers on the basis of an adequacy decision*. Retrieved from EU GDPR: https://gdpr-info.eu/art-45-gdpr/

EU Regulation 2016/679. (2016). Regulation 2016/679 of the European Parliament (General Data Protection Regulations). Retrieved September 10, 2018, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

European Commission v Federal Republic of Germany , Case C-581/07 (Court of Justice of the European Union 2010).

European Data Protection Board. (2019, June 4). *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679.* Retrieved from European Data Protection Board: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf

Federal Trade Commission Act. (2010). Retrieved September 24, 2018

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. (2013). *Report of the Financial Sector Legislative Reforms Commission.* New Delhi: Government of India.

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://poseidon01.ssrn.com/delivery.php?ID=599110006119023029100105026100104117063092005021001065087073074018066029125127107005050023002057007036006022096027103093116072037018087036085028112084014084099004001013081116003086115017113002107112119006117087 0

Hanretty, C., & Koop, C. (2012). Measuring the formal independence of regulatory agencies. *Journal of European Public Policy*, 198-216. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/13501763.2011.607357

India, G. o. (Retrieved February 2020). *Right To Information Act.* . Retrieved from Right to Information: A Citizen Gateway: https://rti.gov.in/rti-act.pdf

Information Commissioner's Office. (2018, September 24). *Principle (a): Lawfulness, fairness and transparency*. Retrieved from UK Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

Information Commissioner's Office. (n.d.). *What is the 'legitimate interests' basis?* Retrieved from UK Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/

Jain, M., & Jain, S. (2013). *Principles of Administrative Law* (7 (Updated) ed.). New Delhi: LexisNexis.

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

Koop, C., & Hanretty, C. (2017). Political Independence, Accountability and the Quality of Regulatory Decision-making. *Journal of Comparative Political Studies*. Retrieved from https://journals.sagepub.com/doi/10.1177/0010414017695329

Krishnan, K., & Burman, A. (2019). Statutory Regulatory Authorities. In D. Kapur , & M. Khosla, *Regulation in India: Design, Capacity, Performance* (pp. 339 - 357). New Delhi: Bloomsbury India.

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

OECD. (2013). Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013) . In OECD, *The OECD Privacy Framework* (pp. 19 - 38). Paris: OECD.

OECD. (2014). *Governance of Regulators*. Retrieved from https://www.oecd-ilibrary.org/docserver/9789264209015-8-en.pdf?expires=1580879281&id=id&accname=guest&checksum=222149EE26231E86A9F74E9105F7687A

Office of Consumer Affairs, Canada. (2010, September 03). *Voluntary Codes Guide- What is a Voluntary Code?* Retrieved from Office of Consumer Affairs, Canada: https://ic.gc.ca/eic/site/oca-bc.nsf/eng/ca00963.html

Office of Parliamentary Counsel, Australian Government. (2019, July). *OPC Drafting Manual.* Retrieved from Office of Parliamentary Counsel, Australian Government: https://www.opc.gov.au/sites/default/files/s05pq37.v27_0.pdf

Office of the Australian Information Commissioner. (2018). *Australian Privacy Principles guidelines.* Retrieved September 4, 2018, from https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/APP_guidelines_complete_version_2_March_2018.pdf

Office of the Parliamentary Counsel, United Kingdom. (2018, July). *Drafting Guidance.* Retrieved from Office of the Parliamentary Counsel: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727629/drafting_guidance_July_2018.2..pdf

Office of the Registrar General & Census Commissioner of India. (2015). *Table C8, Census of India 2011*. Retrieved September 24, 2018, from http://www.censusindia.gov.in/2011census/C-series/C08.html

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/

Prasad, S., Raghavan, M., Chugh, B., & Singh, A. (2019, October 3). *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: https://www.dvara.com/research/wp-content/uploads/2019/10/Policy-Brief-Implementing-the-Personal-Data-Protection-Bill-in-India.pdf

Raghavan, M. (2020). Data Protection in the Information Society: Meeting India's Regulatory Capacity Challenge (forthcoming). In A. Gaur, & A. Sengupta, *Data Democracy – Essays on law and policy in India's digital economy (forthcoming).* New Delhi: Oxford University Press.

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

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

Reserve Bank of India. (2014, May 14). *Notification on Opening of Bank Accounts in the name of Minors*. Retrieved from Reserve Bank of India: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=8872&Mode=0

Reserve Bank of India. (2016). *The Banking Ombusman Scheme.* Mumbai.

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

Rhodia International Holdings Ltd v. Huntsman International LLC, [2007] EWHC 292 (Comm). (n.d.).

Rosenbaum, K. L. (2007, February). *Legislative Drafting Guide: A Practitioner's View.* Retrieved from Food and Agriculture Organisation: www.fao.org/3/a-bb097e.pdf

Roy, S., Shah, A., Srikrishna, J., & Sundaresan, S. (2019). Bilding State Capacity for Regulation. In e. b. Khosla, *Regulation in India: Design, Capacity, Performance* (pp. 360-388). N. Delhi: Bloomsbury.

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, G. (2019). *Principles of Statutory Interpretation.* Lexis Nexis.

Singh, M. P. (2003). *V.N. Shukla's Constitution of India 10th Edition.* New Delhi: Eastern Book Company.

Task Force on Financial Redress Agency. (2016). *Report of the Task Force on Financial Redress Agency.* New Delhi.

The Data Protection Bill of Kenya. (2018). Retrieved September 17, 2018, from http://www.parliament.go.ke/sites/default/files/2017-05/Data_Protection_Bill_2018.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

UK Information Commissioner's Office. (n.d.). *Codes of Conduct*. Retrieved from UK ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/

Unique Identification Authority of India. (2019, July 24). *THE AADHAAR AND OTHER LAWS (AMENDMENT) ACT, 2019.* Retrieved from Unique Identification Authority of India: https://uidai.gov.in/images/news/Amendment_Act_2019.pdf