Protecting the Data

A Comparative Analysis of Pakistan's Personal Data Protection Bill, 2020

MediaMatters forDemocracy
Policy Research & Advocacy Initiative

Protecting the Data

A Comparative Analysis of Pakistan's Personal Data Protection Bill, 2020

Author
Barrister Jannat Ali Kalyar

Edit
Salwa Rana
Hija Kamran
Aimun Faisal

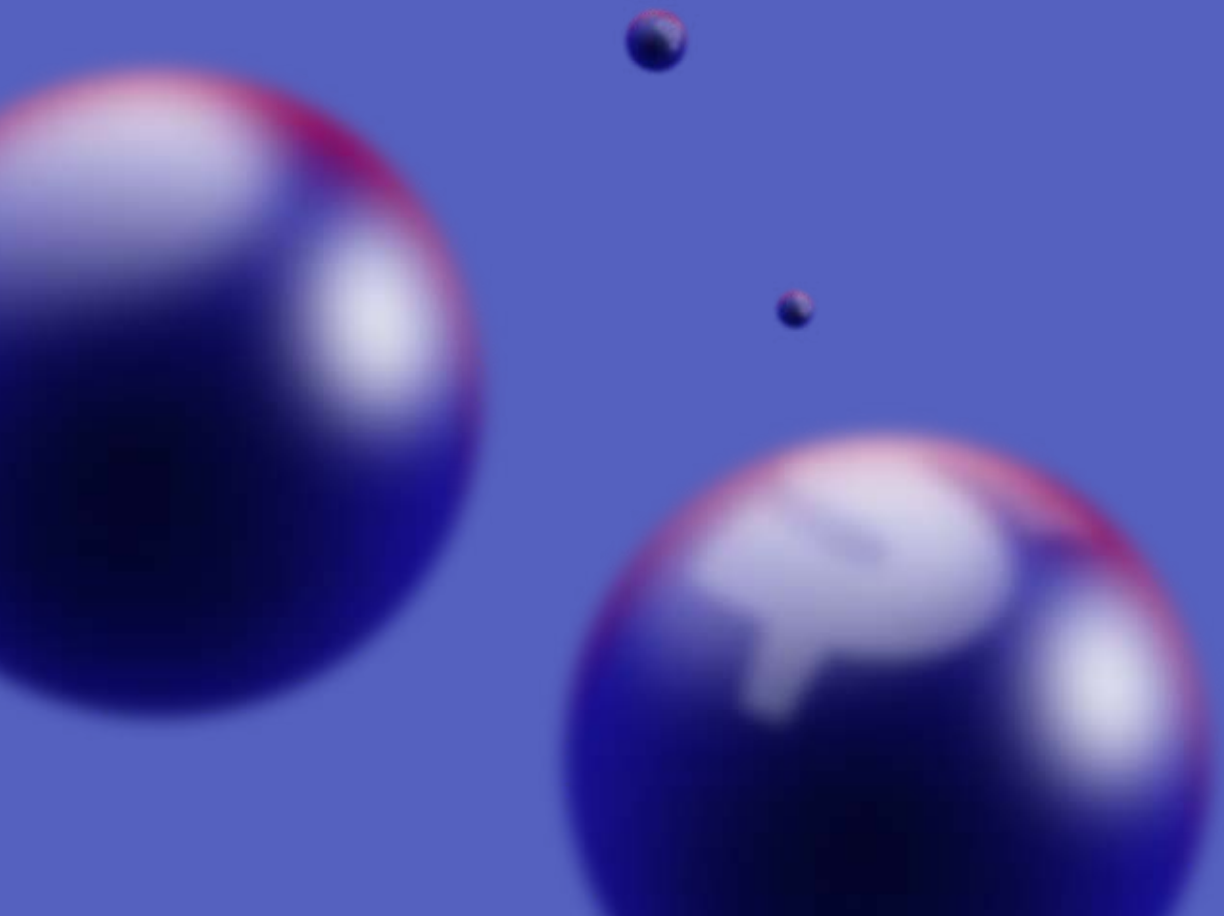
Review
Sadaf Khan
Zoya Rehman

Design and Layout
Aniqa Haider

Published by Media Matters for Democracy in February 2021 under Creative Commons Attribution 4.0 International (CC BY 4.0) https://creativecommons.org/licenses/by/4.0/

MediaMatters forDemocracy
Policy Research & Advocacy Initiative

TABLE OF CONTENTS



EXECUTIVE SUMMARY

The primary reason for a data protection law is to accord protection over citizens' personal data wherever it may be, set up accountability mechanisms for any wrongdoing, and impose clear obligations for public and private data controllers and processors. Lest, the citizens' fundamental rights and freedoms are at the heart of the law, whereby citizens can control the use and access of their data, any such regime would fail to serve its purpose.

While Pakistan's new Personal Data Protection Bill (PDPB), 2020 borrows extensively from the General Data Protection Regulation (GDPR), it still privileges state interests over privacy rights and freedoms of the citizens, potentially allowing for indiscriminate violations of the said rights.
This research identifies significant commonalities and differences between the PDPB and the Indian Data Protection Bill (IDPB), 2019, that, at the time of writing this report, is being debated before the Joint Parliamentary Committee in India. It would be worthwhile to note how the Indian Data Protection Bill commits to protect user data considering its massive population and operating in a rapidly developing country, also home to the world's largest biometric database, Aadhar.

It further discusses best practices from the current international gold standard for privacy i.e. GDPR, that introduced the world's toughest data protection regime. The research also examines the robust UK Data Protection Act (DPA), 2018, that adopted many of the GDPR's standards and even though not as stringent as the EU regulation, is still a comprehensive document that the PDPB must emulate in order to guarantee adequate data protection to Pakistani data subjects, in addition to a secure digital economy for local and international businesses.

Based on the comparison of the four legislations, the following are some of the major recommendations that this research proposes:

1. **The definition of "government"** as controller or processor in the PDPB should be revised to include attached departments, autonomous bodies, parliamentary bodies and other public bodies and authorities to expand the application of the law to any public body that holds citizens personal data.

2. **A more robust and accountable data protection regime** should be incorporated in the PDPB, similar to the DPA that deals with processing for law enforcement purposes, and extends its protection to the processing of personal data by intelligence services and their processors.

3. Clause 5 of the PDPB must provide guidance in relation to the manner in which **informed consent** is to be obtained, particularly the processing of personal data belonging to minors and those incapable of giving consent.

4. The PDPB should also avoid placing unnecessary reliance on consent as a ground for processing, especially in the context of **automated decision-making and profiling,** as often the data subject does not fully understand what they are consenting to and to what extent, and has various other technicalities when a minor data subject is involved. It must also grant the right not to be subject to a decision based solely on automated processing, including profiling as laid down in article 22 of the GDPR.

5. The requirement under clause 23 of the PDPB to withdraw consent through a written notice should be revised, because it excludes those who are unable to furnish a written notice and places unjustifiable burden on the subject. The responsibility should instead be shifted to the controller

to provide assistance to those who are faced with such hurdles and limitations, and simplify the manner in which consent can be withdrawn, at any time. For instance, GDPR mandates the data controllers to enable withdrawing consent through a process which is as simple as the process used to opt-in to data processing; a process that should be one-step and does not require the subject to engage in lengthy written requests and is automated through online platforms.

6. Clause 29 of the PDPB should be removed, and controllers must be obligated to obtain consent each time personal data is collected, and any further processing should be subject to the same standard of fair and lawful processing.

7. Clause 32 is extremely broad in exempting sensitive and critical personal data for certain purposes. It needs to be narrowed down and safeguards and qualifications should also be included to protect against its misuse by public authority.

8. Clause 31 provides sweeping powers to the Federal Government without any parliamentary scrutiny. This contravenes with the fundamental constitutional principle of separation of powers and allows the Federal Government to make arbitrary exemptions in excess of their powers. Therefore, it should be revised to make any rules proposed by the Federal Government subject to the active approval of the Parliament.

9. Clause 20(1) of the PDPB should be revised to obligate the controller to notify a personal data breach if such notification is not impossible or does not involve disproportionate effort. It is crucial that the standards are lowered to "commercially reasonable steps" and other similar exceptions in the GDPR are incorporated.

10. Blanket exemptions in Clause 15 such as *"strategic interests"* of the State should be removed to avoid the arbitrary use of this provision.

11. It is imperative that the Authority is completely separated from the Federal Government for it to enjoy *"complete independence"* in line with recital 117 of the GDPR. Therefore, the requirement under clause 32 that places the Authority under the administrative control of the Federal Government must be removed. Further, sub-clauses that vest sweeping powers in the Federal Government in relation to appointments, directions, exemptions and financial assistance must also be removed.

12. Provisions that authorise the Federal Government to nominate and increase members of the Authority, nominate chairman, remove members, prescribe their qualifications, payment of salary and mode of appointment should be removed, and a more democratic and consultative process must be adopted that is subject to parliamentary approval.

13. The requirement under clause 41(3) to give unfettered control and access to the Federal Government to any return, statement, estimate, statistics or other information in respect of any matter under the control of the Authority or a copy of any document in the custody of the Authority should also be removed.

INTRODUCTION

Over the past few years, there has been a sweeping transition towards the adoption of data protection laws all over the world. Europe's General Data Protection Regulation (referred henceforth as the "GDPR")[1] albeit not perfect, provides the international gold standard by which countries can accord protection to citizens' personal data whilst effectively holding public and private data holders accountable for any wrongdoing.

In the face of countless data leaks at the hands of public and private bodies in Pakistan including the 2019 theft of personal data held by major banks[2] and other major data breaches detailed further in the analysis below, Pakistan has failed to enact a substantial law that affords protections over citizens' personal data.

The Prevention of Electronic Crimes Act 2016 (referred henceforth as "PECA")[3] - a primary legislation that indirectly governs data protection - contains a number of provisions that criminalise unauthorised access to or interference with an information system however, not from a privacy standpoint. Neither does it impose a positive obligation on the controller of the data to ensure the subject's data privacy as is required under a data protection regime.

While article 14[4]of the Constitution guarantees the right to privacy as a fundamental constitutional right, it has still not been recognised as a protected and overriding constitutional right despite it being anchored in human dignity as its founding value.

In line with the global trend, Pakistan is now seeking to enact a federal data protection law that is very similar to the regulations laid down in the GDPR. The Ministry of Information Technology and Telecommunication (MOITT) introduced the new Personal Data Protection Bill (referred henceforth as "the PDPB" and "the Bill") in April 2020.[5]

Seeing that this recent iteration draws extensively from the European model which is anchored in fundamental rights, the impact is mostly positive as it contains all of the data subject rights (minus right to data portability) laid down in the GDPR. However, comparably, the PDPB is restrictive in its material scope as it largely excludes personal data held by public bodies from its protection and affords excessive powers and control to the federal government in key areas, undermining the very purpose of the Bill.

The UK Data Protection Act 2010 (referred henceforth as "the DPA")[6] comes to mind. It incorporates the full scope of the GDPR and further extends its protection to data processed for law enforcement purposes. A regime that must be emulated in the PDPB as will also be discussed in detail below.

The PDPB may be a step in the right direction however it is plagued with the same issues present in the

1. Official legal text. (2019, September 02). https://gdpr-info.eu/
2. Kalyar, J. A. (2019, December 29). Cyber Insecurity. The News on Sunday. https://www.thenews.com.pk/tns/detail/586618-cyber-insecurity
3. Prevention of Electronic Crimes Act, 2016, National Assembly Pakistan http://www.na.gov.pk/uploads/
4. Chapter 1: "fundamental rights" of Part II: "FUNDAMENTAL rights and principles of policy". http://www.na.gov.pk/uploads/documents/1549886415_632.pdf
5. Personal Data Protection Bill, 2020, Consultation Draft V.09.04.2020, Ministry of Information Technology and Telecommunication (MoITT) https://www.moitt.gov.pk/SiteImage/Downloads/Personal%20Data%20Protection%20Bill%202020%20Updated.pdf
6. Data Protection Act 2018. UK https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Bill's last two iterations and more recently the Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2020 (henceforth referred to as "the Rules") that were notified in November, 2020.[7]

The Rules pose a significant threat to the safety of user data by introducing several obligations for social media companies. For instance, Rule 6(6) makes it mandatory for service providers and social media companies to retain information including traffic data linked to the blocked content if asked by the PTA. While this goes beyond the scope of section 37 of the PECA, the parent Act under which the Rules were notified, it also contradicts the protections laid down in PDPB with respect to the retention of user data.

Furthermore, Rule 9(5)(d) states that social media companies and global service providers must establish one or more database servers in Pakistan. Rule 9(7) also requires that social media companies provide decrypted and readable data to the Investigation Agency (in this case, the FIA). These data localisation requirements will make it extremely difficult for a data protection law to operate smoothly and guarantee the effective safeguarding of user data.

As indicated in the statement issued by AIC,[8] the global social media companies are likely to resist and 'reassess their presence' in Pakistan if need be, a situation that might cost Pakistan a massive setback to its digital economy.

In addition, given the history of abuse of power by local law enforcement authorities, locally hosted personal data may be more vulnerable than data hosted elsewhere.

There is no indication of how this data will be used, how long it would be retained, and/or why it is being collected. Given the lack of a data protection law, non-existent transparency, and history of targeting citizens who are vocal online, this clause under the Rules may lead to abuse of power and targeted intimidation of citizens who use the Internet for information.

While the legal framework that the authorities are attempting to set up in Pakistan to regulate the internet and people's digital data in the country contradicts itself, it is imperative to analyse how it compares with the legislations in other countries. Comparable to the PDPB is the latest iteration of the Indian Data Protection Bill (2019) (henceforth referred to as "IDPB").[9] It is equally absurd in its application to public bodies and accords similar discretionary powers to the state and contains wide-ranging exemptions further limiting the scope of the Bill.

This research identifies significant commonalities and differences between the PDPB and the IDPB, and best practices from GDPR, currently seen as one of the best and robust legislative frameworks for data protection. This research also proposes recommendations in relation to expanding the material scope and application of the PDPB, revising the definitions contained therein, bringing more clarity to the grounds to processing of personal data and sensitive personal data and the rights of data subjects including granting data subjects the right to compensation, and revising the structure and composition of the data protection authority to make it more transparent, independent and accountable.

7. Social Media Rules. Ministry of Information Technology and Telecommunication, Pakistan. https://moitt.gov.pk/SiteImage/Misc/files/Social%20Media%20Rules.pdf
8. [Pakistan] AIC Issues media statement on new Internet RULES (20 Nov 2020). https://aicasia.org/2020/11/20/pakistan-aic-issues-media-statement-on-new-internet-rules-20-nov-2020/
9. Ministry of Electronics & Information Technology, India. (2018). [INDIA] THE PERSONAL DATA PROTECTION BILL, 2018. https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

ANALYSIS

I. Scope and Applicability

Defining "government", "state", "authorities"

The PDPB purportedly emphasises its application to private organizations in the exercise of processing personal data of Pakistani citizens within and outside the country. However, it is unclear if the processing of personal data by public bodies would warrant the same level of protection. Clause 2: Definitions only vaguely mentions *"government"* as a category of controller and processor, and leaves it open to interpretation.

Given that most of the citizens' data resides within government-held databases such as the National Database and Registration Authority (NADRA), the Bill should spell out what the term means and the bodies that fall within its ambit. This has also been seen in drafts proposed in other countries. For instance, the mention of *"state"* as a category of controller or processor in the IDPB is equally ambiguous. These vague terms should be defined to include attached departments, autonomous bodies, parliamentary bodies and other public bodies and authorities to limit how they are interpreted.

Extending protection to "data processed for law enforcement purposes"

Another contention is that the processing of personal data by authorities with law enforcement functions is not protected under the PDPB. While the GDPR does not address this, Part 3 of the DPA, based on a separate EU directive on law enforcement processing, specifically sets out a data protection regime for authorities when they are processing for law enforcement purposes. It defines law enforcement purposes as, *"the prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."*[10]

This is particularly relevant for whenever law enforcement bodies deploy surveillance technologies in public spaces "for crime prevention". For example, the "Hotel Eye Software" of the Peshawar Police is used to access the data of visitors who stay at hotels which is then fed into their database, on a daily basis.[11]

This raises serious concerns since it involves the use of personal and sensitive personal data by a law enforcement body that must be subject to the same data protection regime as provided in the DPA. In any event, such indiscriminate surveillance would not qualify as a general or law enforcement purpose, and would be in gross violation of the core principles[12] laid down in the GDPR and are also reflected in the United Nations Principles of Data Protection and Privacy passed in 2018.[13]

10. Data Protection Act 2018. UK https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
11. The News. (2019, January 15). Peshawar Police launch 'Hotel Eye' software. https://www.thenews.com.pk/print/419236-peshawar-police-launch-hotel-eye-software
12. The principles. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/
13. United Nations. (2018). UN Principles on Data Protection and Privacy. https://archives.un.org/sites/archives.un.org/files/_un-principles-on-personal-data-protection-privacy-hlcm-2018.pdf

Listing "competent authorities"

The DPA also lists *"competent authorities"* to carry out law enforcement functions in its Schedule 7 and extends it to processors *or any other person having statutory functions to exercise public authority or public powers for law enforcement purposes.*

Although, no separate section is dedicated to law enforcement processing in the PDPB, and there is no mention of any investigation or law enforcement bodies equivalent to those listed in the DPA, and if they fall within the ambit of the law. However, the Statement of Objects of the PDPB discusses the role of PECA in its application, that designates the FIA as the investigation body *"for the purposes of criminal investigation or criminal proceedings."*

PECA empowers an authorized officer of the FIA to acquire data (s.31), apply for warrant for search or seizure (s.33), apply for warrant for disclosure (s.34), acquire information or data in unencrypted or decrypted intelligence format (s.35), and request real time collection of data (s.36).

The illusory safeguards provided in these sections fall short of the bare minimum standard or protection provided in the PDPB. Therefore, it is imperative to extend the scope of the PDPB to the FIA and other *"competent authorities"* conducting law enforcement processing to protect citizens' data. This would subject the FIA to the same test of fair and lawful processing in line with the principles of the GDPR that are also specifically written into Part 3 of the DPA, concerning law enforcement processing. Corresponding to the PDPB, the IDPB also does not subject law enforcement bodies to a similar legal regime.

Social media intermediaries, profiling

Further, clause 3: Scope and Applicability of the PDPB extends its application to any natural or legal person (local or foreign) located in Pakistan, *who processes or has control over or authorizes the processing of any personal data.*

It also requires data controllers and processors not established or registered in Pakistan to nominate a representative in the country. However, it does not specify whether this requirement applies indiscriminately to all controllers or processors dealing with personal data of Pakistani subjects outside its terriroty or just the social media companies.

This is deeply concerning particularly because comparable data localisation provisions in Online Harm Rules were used to coerce social media companies to nominate representatives and establish permanent registered offices in the country (Rule 9(5)).[14] In this vein, the PDPB would also be misused to pressure social media companies to comply with the Government. In addition to curbing online freedoms, data localisation poses serious economic threats to the country's digital economy and has no place in a data protection law. (More on data localisation and cross-border transfer discussed later in this report.)

On the contrary, the GDPR effectively extends its protection to personal data of EU members and their citizens within and outside its territory. Instead of requiring data to be localised, it prohibits and restricts transfer of data to countries or organisations that do not provide adequate data protection.

Further, article 3 of the GDPR expands its application to *the monitoring of behaviour of members that takes place within the EU and in relation to the offering of goods or services, irrespective of whether a payment of the data subject is*

14. Pakistan Telecommunication Authority. (2020). Removal and Blocking of Unlawful Online Content (Procedure, Oversight, Safeguards) Rules, 2020. https://www.pta.gov.pk/assets/media/notification_sro_18112020.pdf

required, to such data subjects in the EU. The PDPB should adopt a similar approach that expands the protection of the law to different categories of citizens' personal data, wherever they may be located rather than arbitrarily limiting its application to a selected few.

Additionally, clause 26 of the IDPB narrowly defines "social media intermediary" with its focus on giant social networking sites. It states that a social media intermediary should not process sensitive personal data such as genetic data or biometric data, or any other data that could cause harm unless it has undertaken a data protection impact assessment in accordance with the provisions of this section. However, the PDPB does not mention social media intermediary as a separate category of controller or processor nor does it contain similar provisions to address the privacy concerns arising from automated decision-making and profiling.

As per article 4 of the GDPR, *profiling "means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."*

This is also written into section 33 of Part 2 of the DPA, and must also be incorporated in the PDPB as a fundamental right because it would provide more safeguards to subjects who would be in a better position to decide if they want to give consent. This would essentially prohibit companies from processing certain information without the subject's consent, that could potentially be used to profile and classify them which is typically the case in targeted advertising.

Sensitive Personal Data

Furthermore, with the restrictive definitions contained in clause 2: Definitions of the PDPB, particularly in relation to sensitive personal data, it would be impossible to fully realise the rights enshrined in the bill. In comparison, the IDPB provides a more expansive definition of sensitive personal data in line with the GDPR. It categorises *intersex status, transgender status, political beliefs, caste or tribe, genetic data, mental health related data, sexual life* and *sexual orientation* as sensitive personal data. In addition to the types mentioned above, the PDPB should also include *membership of a trade union, economic, cultural or social identity of a natural person and philosophical beliefs,* not included in the IDPB but are protected under the GDPR. Profiling, restriction of processing, official identifier should also be defined and brought under the scope of the bill.

Pseudonymized Personal Data

In addition, the definition of personal data provided in the PDPB also falls short of the GDPR standard that explicitly states in its recital 26 that pseudonymized data is also personal data.

Pseudonymization is a process that lets you replace the original data set with a pseudonym, for example replacing a data subject's name with an alias. **It is important to understand that pseudonymized data can be attributed to a natural person with the use of additional information, and it is a reversible process that also allows for re-identification later once the data is de-identified, unlike anonymization that is not reversible.** Recital 28 encourages the use of pseudonymization to personal data as an added layer of security for subjects' data and helps controllers and processors to meet their data protection obligations.

However, clause 2(b) of the PDPB conflates *"pseudonymization"* with *"anonymization"* thereby excluding both from the categories of personal data and beyond the scope of the PDPB. Furthermore, recital 26 of the GDPR only excludes anonymous information which is no longer identifiable to a natural person and affords its protection to pseudo-anonymized personal data that could be attributed to a natural person by the use of additional information.

Recommendations

- The definitions of controller and processor should be revised in line with article 2 of the GDPR to include public bodies and authorities;
- A separate, more robust data protection regime should be incorporated in the PDPB, similar to Part 3 of the DPA[15] that deals with processing for law enforcement purposes;
- The PDPB should also emulate Part 4 of the DPA that extends its protection to processing of personal data by the intelligence services and their processors;
- Clause 3.2 of the PDPB that requires the nomination of a representative is a gross violation of the fundamental principles laid down in the bill, and therefore must be removed;
- The PDPB should divert its focus to ensuring safe transfer of data by prohibiting and restricting it to countries or organisations that do not offer "adequate" data protection as opposed to data localization;
- The PDPB must also grant the right not to be subject to a decision based solely on automated processing, including profiling as laid down in article 22 of the GDPR;
- Revise the definitions of personal data and sensitive personal data, as per the GDPR;

15. Data protection Act 2018. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

II. Grounds for Processing Personal Data

Consent

The inclusion of the definition of "consent" in the PDPB is a much-needed addition.
Clause 2 defines consent as: *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the collecting, obtaining and processing of personal data relating to him or her."*

It echoes the definition laid down in article 4 (11) of the GDPR that section 84 (2) of the DPA also emulates. Consent is one of the lawful bases for the processing of personal data under the GDPR, and for special category or sensitive personal data, *"explicit"* consent is required to legitimise its use. While the PDPB is anchored in a similar consent model however, its clause 5 provides no guidance on how consent, in particular, explicit consent needs to be obtained.

As per article 8 of the GDPR, obtaining consent is not sufficient, instead it is crucial to also demonstrate that it has been obtained in *a valid, freely given, voluntary, unambiguous and informed manner.*

Since the PDPB version relies heavily on consent as the main legal processing ground, it must detail a process setting out baseline requirements for how consent is to be obtained, particularly of minors and those incapable of giving consent. Whereas, section 8 of the DPA in line with the GDPR, and clause 16 of the IDPB contain a separate section addressing the rights of minor data subjects, but the PDPB remains silent.

Further, placing unnecessary reliance on consent means legitimising processing otherwise restricted, such as automated-decision making (including profiling) or even cross-border transfers by private bodies in the absence of adequate safeguards - solely on the basis of explicit consent. Therefore, it is reiterated that the right not to be subject to a decision based solely on automated processing and profiling be included in the PDPB to ensure that it is subject to adequate safeguards.

Therefore, care must be taken as consent is often not the most appropriate and safest form of processing personal data because it could potentially have very serious implications for subjects. Specially in the absence of effective safeguards for securing meaningful consent and the power imbalance between subjects and controllers, scales will most definitely be tipped against subjects, and consent is likely to be misused to absolve controllers of their responsibilities.

Recommendations

- Clause 5 of the PDPB must provide guidance in relation to the manner in which consent is to be obtained. Particularly, the processing of personal data belonging to minors and those in capable of giving consent must be detailed in the PDPB as explicated in s.8 of the DPA, clause 16 of the IDPB and the GDPR. Currently, it remains excluded from the scope of the PDPB.
- The PDPB should avoid placing unnecessary reliance on consent as a ground for processing, especially in the context of automated decision-making and profiling.

Withdrawal of Consent

As per article 7(3) of the GDPR and its supplementary recitals, the subject shall have the right to withdraw their consent at any time, and it should be communicated to the subject prior to giving consent. Similarly, the PDPB in its clause 23 grants the right to withdraw consent to the processing of personal data. However, it requires the subject to do so through a written notice. This automatically excludes those who are unable to furnish a written notice due to illiteracy or lack of familiarity with the procedure. Additionally, the burden of withdrawal of consent should not be placed on the subject, but should be a positive obligation or requirement on the controller to provide assistance to those who are faced with such hurdles and limitations.

Further, requiring subjects to withdraw through a written notice means it is not possible for them to withdraw consent *"at any time",* on their own initiative, contrary to the GDPR and the DPA. According to these two laws, even an *"opt-out only by reply"* option would be insufficient in this context as it would create an unnecessary hurdle and delay for the subject in exercising this fundamental right.

The UK Information Commissioner's Office further explains it. It states that, *"the key point is that all consent must be opt-in consent, ie a positive action or indication – there is no such thing as 'opt-out consent'. Failure to opt out is not consent as it does not involve a clear affirmative act. You may not rely on silence, inactivity, default settings, pre-ticked boxes or your general terms and conditions, or seek to take advantage of inertia, inattention or default bias in any other way. All of these methods also involve ambiguity – and for consent to be valid it must be both unambiguous and affirmative. It must be clear that the individual deliberately and actively chose to consent."*[16]

Clause 23 of the PDPB further contains a *term of imprisonment not exceeding a year or a fine not exceeding 5 million or both,* if the controller fails to cease the processing of personal data after consent has been withdrawn. On the contrary, under the GDPR and the DPA, the controller would only be liable to pay a fine. Attaching a criminal liability with this section would result in overlaps with other criminal laws, such as the PECA 2016, and would require the establishment of malicious intent *(mens-rea)* on part of the data processors in the Court.

Further, the GDPR is clear that if there exists a penalty for withdrawing consent, the consent would be invalid as it is not freely given and there is a liability attached to the withdrawal of consent. Whereas, subjects must be able to withdraw consent without suffering any detriment. However, clause 11(6) of the IDPB penalises withdrawal of consent, restricts it and renders the subject liable for all legal consequences. It states that, *"where the data principal withdraws his consent from the processing of any personal data without any valid reason, all legal consequences for the effects of such withdrawal shall be borne by such data principal."* This is not only a disincentive but it also calls into questions whether the consent obtained by the subject is free. Fortunately, no such penalty exists in the PDPB.

16. Guide To The General Data Protection Regulation. https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

Recommendations

- The requirement under clause 23 to withdraw consent through a written notice should be revised, because it excludes those who are unable to furnish a written notice and places unjustifiable burden on the subject. The responsibility should instead be shifted to the controller to provide assistance to those who are faced with such hurdles and limitations. In addition, the PDPB should remove the requirement to withdraw consent through a written notice because it would create unnecessary hurdles and delay and simplify the manner in which consent can be withdrawn, at any time. Intead, a one-step electronic mechanism which is as easy and simple as the opt-in method should be set up to assist subjects to withdraw consent.

- The PDPB should not carry a criminal liability as this will result in overlaps with other criminal laws such as Sections 3, 4, 5 and 16 of the Prevention of Electronic Crimes Act 2016 (PECA). It is also important to note that criminal actions require the element of mens-rea (intent) so even if the bill does intend to establish a criminal penalty for violation of such provisions, it should be reserved for the most egregious of violators who committed violations with malice or aforethought.

- Instead of criminal liabilities, financial liability in the form of a statutory compensatory regime should be introduced, which should compensate the aggrieved party (the person(s) who's data has been compromised) without prejudicing that party's right from approaching the civil courts for compensation.

Alternative Grounds to Consent

Mirroring article 5 of the GDPR on alternate grounds of processing,[17] s.6 of the DPA sets out five alternatives to consent for the processing of personal data as follows;

1. *performance of a contract,*
2. *compliance of a legal obligation to which controller is subject,*
3. *protecting vital interests of the data subject or of another natural person,*
4. *legitimate interests pursued by the controller or by a third party, and*
5. *conducting a task carried out in the public interest or in the exercise of official authority.*[18]

The PDPB contains all the legal bases except the last one.

17. Art. 5 Gdpr – principles relating to processing of personal data. (2016, August 30) https://gdpr-info.eu/art-5-gdpr/

18. Data protection Act 2018. UK https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

While, the GDPR recitals 39 to 50[19] provide adequate guidance to controllers in evaluating the appropriate legal ground for processing personal data, it is unclear whether the interpretation of certain borrowed terms, particularly in the PDPB carry the same meaning and interpretation. In particular, sub-clause 5.2 of the PDPB allows processing for "legitimate interests" pursued by the controller.

However, it does not define what these "legitimate" interests are, and fails to include the qualification provided with pursuing legitimate interests as laid down in the GDPR. The qualification in GDPR is that where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child, this ground is not applicable.

Further, Recital 47 of GDPR makes it clear that this ground is not available to public authorities in the performance of their tasks as there exists a separate ground for them to exercise their official authority that is subject to corresponding conditions and legal safeguards. Additionally, in relation to grounds such as for *the exercise of official authority vested in the controller or in the public interest and to fulfil a legal obligation,* the GDPR requires Member States to introduce more specific provisions by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing.

However, the PDPB does not contain comparable provisions, and instead provides another ground that allows *for processing for the exercise of any functions conferred on any person by or under any law.* This ground is loosely worded and is not subject to the same standard of lawful and fair processing as laid down in the GDPR. Given the practice of weaponizing laws against individuals, in particular the marginalised sections of society, by public bodies and law enforcement agencies, this could be extremely dangerous and should be removed at the onset.

Further, the PDPB tailors the GDPR version of the term *"vital interests"* that is essential for the life of the data subject to also include the *"security"* of the data subject. This is an equally problematic provision that is susceptible to abuse particularly by state bodies to justify any incursion in the privacy of the data subject.

Proportionality Test

All the provisions contained within PDPB that allow controllers to process personal data without the consent of the subject must be made subject to the principles of *"necessity"* and *"proportionality"* expounded by the GDPR and DPA as established principles of data protection.

As per the EU case law, necessity is the first step before assessing the proportionality of the restriction, and is essential in assessing the lawfulness of the non-consensual processing. In addition, proportionality, being a general principle of EU law, requires that the measure taken for data protection is adequate to achieve the envisaged objective. This is the test that the Court of Justice of the European Union (CJEU) and UK courts apply to assess the lawfulness of the processing of personal data.

Additionally, in a recent landmark judgment of the Indian Supreme Court in the Puttaswamy case[20] - also known as the right to privacy judgement -Chandrachud J., drawing from the concept of proportionality in the EU jurisprudence, stated that the right to privacy is a fundamental right that is subject to reasonable restrictions, and laid down a three-fold test namely; *(i) existence of law, (ii) legitimate aim,(iii)proportionality of the*

19. Recital 39 - principles of data processing. (2019, September 02). https://gdpr-info.eu/recitals/no-39/

20. Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018, Indian Kanoon, https://indiankanoon.org/doc/127517806/

legitimate aim with the object sought to be achieved. Kaul J., further expanded on the proportionality test relying closely on the European standard. He added the fourth element namely; *(iv) procedural safeguards against abuse of interference with rights.*

Regardless of the significant development of the proportionality test against arbitrary and excessive restrictions and the scope of the privacy right in India, the IDPB still fails to meet even the basic judicial review standard laid down in the majority decision, and makes no mention of the proportionality test or its application anywhere in the law.

Comparably, the PDPB also does not lay down a proportionality test, the application of the principles of proportionality and necessity or any corresponding legal safeguards. It is also important to note that these principles are not established principles in the Pakistani jurisprudence, and this will be an additional hurdle for citizens seeking recourse against the violation of their privacy rights.

In the absence of a proportionality test, the Authority and the Federal Government would be allowed to impinge with impunity on subjects' privacy rights guaranteed under the Bill and the Constitution of Pakistan.

In addition, the PDPB largely ignores the principles in relation to processing laid down in the GDPR, and as incorporated by the DPA. It briefly mentions purpose limitation and data minimisation, and excludes the rest of the fundamental principles including: *lawfulness, fairness and transparency, accuracy, storage limitation, security and accountability.*[21]

Recommendations

- Guidance is required in relation to the meaning and interpretation of *"legitimate interests"* in clause 5.2 of the PDPB, including the qualification provided under the GDPR particularly in the context of a child data subject. It is imperative that this ground is also not misused by public authorities.
- The loosely worded ground *for the exercise of any functions conferred on any person by or under any law* should be replaced with a parallel ground in the GDPR for *the exercise of official authority vested in the controller or in the public interest and to fulfil a legal obligation* as it is subject to precisely specific requirements and measures to ensure lawful and fair processing.
- The definition of *"vital interest"* in clause 2(n) should be revised to exclude security of the data subject.
- All the provisions that allow processing without the consent must be made subject to the principles of necessity and proportionality established in the GDPR, the jurisprudence of the CJEU, and the recent Indian Supreme Court decision on right to privacy.

21. Guide To The General Data Protection Regulation. https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

- The PDPB must fully incorporate and realise the fundamental principles in relation to processing laid down in the GDPR, including, lawfulness, fairness and transparency, accuracy, storage limitation, security and accountability.

Processing of Sensitive Personal Data

Clause 28 of the PDPB enumerates a list of exceptions to "explicit" consent- borrowed from the GDPR - for processing sensitive personal data. While, it does contain some similar provisions as in the GDPR. However, it excludes *processing that is necessary for reasons of substantial public interest to be proportionate to the aim pursued, processing that is carried out in the course of legitimate activities with appropriate safeguards by a foundation etc and processing necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.*

The PDPB vaguely discusses data processing for medical purposes by a health care professional or the equivalent who owes a duty of confidentiality to the subject and defines medical purposes as *preventive medicine, medical diagnosis, medical research, rehabilitation and the provision of care and treatment and the management of health care services.*[22]

However, it does not contain a provision that allows for processing of sensitive personal data in the public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices. It also does not introduce any further conditions or limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Further, as per the DPA, processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent. However, the PDPB does not provide rationale on what it means *by consent cannot be given or on behalf of the data subject" and "the data controller cannot reasonably be expected to obtain consent from the data subject.*[23]

Recommendations

- Clause 28 of the PDPB should include a provision that allows for processing of sensitive personal data in the public interest in the area of public health in addition to archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. It should also include any further conditions or limitations, with regard to the processing of genetic data,

22. Clause 28 of the Personal Data Protection Bill (2020) Pakistan https://moitt.gov.pk/SiteImage/Misc/files/Personal%20Data%20Protection%20Bill%202020(3).pdf

23. Personal Data Protection Bill (2020) Pakistan https://moitt.gov.pk/SiteImage/Misc/files/Personal%20Data%20Protection%20Bill%202020(3).pdf

biometric data or data concerning health.

- The PDPB should also provide rationale and clarity on what it means by *"consent cannot be given or on behalf of the data subject"* and *"the data controller cannot reasonably be expected to obtain consent from the data subject."*

III. Exemptions

Repeated Collection

Clause 29 of the PDPB absolves controllers from the obligation to obtain consent for repeated collection of personal data, referred to as "subsequent collection", if not more than twelve months have passed between the "first collection" and the "subsequent collection." This is incompatible with the objective of the PDPB and the definition of consent enshrined in article 4 of the GDPR and the PDPB. It also deviates from the core principle of "purpose limitation" by providing a blanket exemption to controllers to obtain personal data for one purpose and then use it for other purposes, without notice - a mandatory requirement under clause 6 of the PDPB - including the option to withdraw consent. Therefore, clause 29 must be removed as any further processing should be subject to the same standard of fair and lawful processing.

Other exemptions

Clause 32 of the PDPB deviates from article 2 of the GDPR by introducing extremely broad exemptions that further exclude from its scope, sensitive and critical personal data required for *apprehension of offender, assessment of collection of any tax or duty or any imposition of a similar nature and for the purpose of discharging regulatory functions. All three exemptions are extremely vague and are left open to interpretation.* They are susceptible to abuse by public authorities performing these tasks. Therefore, they must be made subject to even more specific requirements for processing and corresponding legal safeguards to ensure lawful and fair processing.

Further, clause 32 also authorises the processing of data for research and collection of statistics without the consent of the subject. However, it provides no legal safeguards against the use of personal data for the purpose of profiling. This is a cause of concern especially because personal profiles are used as a tool for targeting through political advertisements. Cambridge Analytica being the most prominent example. It is also important to note that even if the data is being processed for such specified purposes it must still be required to comply with the provision of fair and reasonable processing. It is reiterated that subjects must have the right not to be subject to a decision based solely on automated processing and profiling, which could significantly affect them or have legal effects concerning them. This is a right enshrined in article 22 of the GDPR and must be written into the Bill.

Power to make further exemptions

As per clause 31, the Federal government is empowered to make further exemptions and impose any terms or conditions as it thinks fit. This poses a serious threat to the independence of the authority that is tasked with holding the government and private bodies to account and therefore must be completely independent from any government control. Further, the sweeping powers vested in the Federal Government would allow excessive delegation and exemption from any parliamentary oversight or scrutiny. In this regard, the recently passed Rules i.e. Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguard) Rules, 2020 serve as a useful reminder. In comparison, s. 16 of the DPA authorises the Secretary of State to make further exemptions by way of regulations subject to the affirmative resolution procedure, meaning it must be actively approved by both Houses of Parliament. However, similar to the PDPB, chapter 8 of the IDPB vests sweeping powers in the Central Government to exempt any body of government from application of the Act (clause 35) and exempt certain data processors (clause 37). PDPB thus appears to be following a flawed example set by IDPB, rather than working with the rigorous framework introduced by GDPR and DPA.

Recommendations

- Clause 29 of the PDPB should be removed and controllers must be obligated to obtain consent each time personal data is collected and any further processing should be subject to the same standard of fair and lawful processing.

- The PDPB should also not deviate from the principle of "purpose limitation" by providing a blanket exemption to controllers to obtain personal data for one purpose and then use it for other purposes.

- Clause 32 is extremely broad in exempting sensitive and critical personal data for certain purposes. It needs to be narrowed down and safeguards and qualifications should also be included to protect against its misuse by public authority.

- Clause 31 provides sweeping powers to the Federal Government without any parliamentary scrutiny. This contravenes the fundamental constitutional principle of separation of powers, and allows the Federal Government to make arbitrary exemptions in excess of their powers. Therefore, it should be revised to make any rules proposed by the Federal Government subject to the active approval of the Parliament.

IV. Powers of the Federal Government

Under the PDPB, the Federal Government is commissioned to

- Notify certain categories of personal data as exempt from the requirement for cross-border transfer on the grounds of necessity or strategic interests of the State (clause 14)
- Prescribe upon recommendation of the Authority such cases where clause 25 (right to prevent processing likely to cause damage) will not apply, give express authorization in accordance with the procedure to be laid down in relation to the exemption for journalistic expression (clause 30)
- Establish Authority under its administrative control and appoint seven-member committee of the Authority
- Increase the number of members of the Authority and prescribe their qualifications and mode of appointment, nominate chairman, determine their salary and remuneration, accept resignation and remove any member (clause 32)
- Direct the Authority to perform functions from time to time (clause 33)
- Direct any other Member to serve as acting Chief Data Protection Member if the position of chairman is vacant (clause 37)
- Issue policy directives to the Authority that must be complied with (clause 38)
- Determine the manner in which accounts will be kept (clause 39), its liability to be limited to the extent if any grant made or loan raised (clause 40), issue loans and grants including the initial grant
- Give approval for co-operation with international organisations, give approval to Authority to make rules (clause 48)
- And remove any difficulties in relation to the provisions in the Act within two years of the commencement (clause 50).

Recommendations

- These powers undermine the entire framework of the proposed legislation in light of the lack of independence of the Authority and the accountability that the Federal Government owes to the subjects and the Parliament. Therefore, they must be removed.

V. Rights of Data Subjects

Right to Data Portability

Article 68 of the GDPR provides the right to data portability that essentially allows the subject to *"receive personal data in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller."* Recital 68, further states that this right must apply where the data is carried out by automated means and only on the basis of consent or contract. Clause 19 of the IDPB contains a comparable provision however it does not exist in the PDPB, and therefore it will be valuable to incorporate it.

Right of Access to Personal Data

Clause 16 of the PDPB entitles subjects to be informed whether their data is being processed by or on behalf of the controller. Clause 17 of the IDPB lays down a comparable right called the *"right to information and access."*

Exercising this fundamental right should not be contingent on the payment of a prescribed fee charged by the controller. This requirement should be removed from clause 17 of the PDPB as it is contrary to article 15 of the GDPR that only allows the controller to charge a "reasonable fee" based on administrative costs for "further" copies.

Further, it does not prescribe the minimum information the subject should be provided with, in addition to a copy of their data. Article 15 of the GDPR and its supplementary recital 63 provide that the following information is to be made available to the subject in response to their request: *the purpose of processing, the categories of the data, the named recipients with whom the data has or may be shared, the period of retention, the source of the data, their rights in relation to the data, any transfers of the data to third countries and the safeguards in place, existence of profiling and the consequences, the existence of automated-decision making, and meaningful information about the logic, significance and consequences.*

These must be incorporated in the PDPB, and instances of automated decision making and profiling should also be addressed. There is no accountability and transparency in relation to automated decision making in both the IDPB and the PDPB, and they must be written into the list of rights. In contrast, the GDPR takes a more expansive approach called the right to explanation. This involves a combination of rights to access, notification requirements and safeguards against automated decision making.

Further, article 19 of the GDPR obligates the controller to notify relevant persons of the rectification to the personal data. Clause 20(1) of the PDPB and clause 18(4) of the IDPB impose a similar obligation. However, both the clauses provide no exceptions contained in the GDPR that require this obligation to be met only if such notification is not impossible or does not involve disproportionate effort. Therefore, standards should be lowered to "commercially" reasonable steps or similar exceptions as provided in the GDPR as both the bills in their current form only add to the compliance requirements of the controller that are obligated to comply with them for all processing by and on its behalf.

Right to Correct Personal Data

Article 16 of the GDPR states that the subject shall have the right to obtain from the controller, without undue delay, the rectification of inaccurate personal data concerning them. However, clause 19 of the PDPB requires the subject to make a data request in writing and provides up to thirty days to the controller to respond to the subject's request. There are similar flaws in clause 18 of the IDPB, which does not even provide a deadline by which the controller must comply with the subject's request. Both the provisions fall short of the GDPR's standard that requires the rectification without undue delay. It further states that the subject is also entitled to have incomplete personal data completed, including by means of providing a

supplementary statement.

Right to Erasure

Clause 27 of the PDPB provides the right to erasure of personal data without undue delay and obligates controllers to erase personal data within 14 days where it is no longer necessary, where subject's consent was withdrawn and it was the only available ground, it has been processed unlawfully or in compliance with a legal obligation. In comparison, clause 18 of the IDPB is limited in its scope as the right to erasure is available only if the personal data is no longer necessary for processing. This contravenes with recital 65 of the GDPR that contains all the conditions also provided in the PDPB.

Further, article 18 of the GDPR states that in case of any dispute regarding the accuracy of data, the data subject has the right to restrict processing. It means the marking of stored personal data with the aim of limiting their processing in the future. However, the rights of data principals are diluted under the PDPB as a comparable provision does not exist.

Clause 27 (3) of the PDPB is in line with the GDPR that states that the further retention of personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

In addition, this right is particularly relevant where the subject is a minor or not fully aware of the risks involved when they gave consent to process their data and they would now want to remove such personal data, especially on the internet.

It is important to note that the right to erasure and to be forgotten can be extremely complicated in the context of new technologies where individual data is used to generate new inferences, and could potentially affect individuals even after their personal data has been erased. Therefore, it is crucial that subjects are aware of automated decision making, and are given the choice to opt-out, especially in public systems. This would not only ensure transparency and accountability but would also protect subjects from discriminatory outcomes.

Recommendations

- The PDPB should emulate the right to data portability laid down in article 68 of the GDPR.
- The requirement to pay a prescribed fee to the controller should be removed from clause 17 and conditions contained in article 15 of the GDPR incorporated accordingly.
- It should prescribe the minimum information the subject should be provided with as laid down in article 15 and recital 63 of the GDPR.

- Clause 20(1) of the PDPB should be revised to obligate the controller to notify a personal data breach if such notification is not impossible or does not involve disproportionate effort. It is crucial that the standards are lowered to "commercially reasonable steps" and other similar exceptions in the GDPR are incorporated.

- Clause 19 of the PDPB falls short of the GDPR's standard in article 14 that requires the rectification without undue delay, and its requirement to furnish a data rectification request in writing must be removed.

- Clause 27 should be revised to include the right to restrict processing in the event of a dispute regarding the accuracy of the information as provided in article 18 of the GDPR. The controller should also be obligated to erase the data without undue delay.

VI. Cross-Border Transfer

In July 2020, the Court of Justice of the European Union (CJEU) struck down the EU-US Privacy Shield[24] that allowed companies to self-certify and commit to a framework agreement to transfer data to the US. It was invalidated because the US laws failed to ensure compliance with the level of protection required by GDPR. This serves as a useful example particularly in the context of the PDPB that grossly violates the GDPR's framework for cross-border transfers.

As per clause 14 of the PDPB, personal data can be transferred upon obtaining consent if the country it is being transferred to, provides *"adequate"* data protection, at least equivalent to the protection provided under the PDPB.

However, it does not state if adequacy will be assessed by the Authority or the Federal Government, neither does it provide other alternatives nor does it address what will happen in the absence of an "adequacy decision". Additionally, clause 15 states that the transfer of personal data will be subject to a framework that will be devised by the Authority subsequently. It also identifies *"necessity"* or *"strategic interests"* of the State as grounds that can be used by the Federal Government to restrict the international transfer of certain other categories of personal data.

On the contrary, in the GDPR context, the *"adequacy decision"* is a finding by the EU Commission that assesses the legal framework in place in that country or international organisation that provides adequate protection for individuals' rights and freedoms for their personal data. Additionally, in the absence of an adequacy decision or other appropriate safeguards detailed in the GDPR, it also provides alternate conditions under which a transfer can take place.

Further, in addition to restricting the processing of critical personal data within the local servers or data centres of the country, clause 15 of the PDPB also mandates the Authority to devise a mechanism for keeping a copy of personal data in Pakistan. This is alarming especially in light of the abuse and weaponization of PECA to clamp down on online freedoms coupled with the passage of the Rules that also obligate the social media companies to set up their servers in Pakistan and provide access to unencrypted and decrypted data to the authorities as and when demanded. It is particularly telling of the intention behind the Bill.

Further, this requirement under PDPB is also contrary to s.34 of PECA that requires a court warrant for the disclosure of content data. In addition, due process requires the subject to be notified if their data is required by the government and they should be given the chance to oppose that.

While the State may require access to certain types of data for counter-terrorism or other purposes for crime-prevention, however, data localisation is not a method that democracies use to get that information as there exist Mutual Legal Assistance Treaties (MLAT) and other mechanisms that can be used for information sharing between states. The countries that localise data, use it to prosecute and censor speech, and it has nefarious consequences for speech. Therefore, in the absence of an independent data protection authority and a "reasonably-minded" judiciary to regulate against arbitrariness, it is best to remove these provisions.

24. BBC. (2020, July 16). EU-US Privacy Shield for data struck down by court. https://www.bbc.com/news/technology-53418898

The IDPB contains comparable provisions that require critical personal data and sensitive personal data to be localised, and critical personal data to be transferred only for emergency processing or subject to an adequacy decision. Contrary to the PDPB, it prescribes additional requirements, an adequacy test, or specific approval by the data protection authority. It also requires certain social media intermediaries to provide users the option to voluntarily verify their accounts.

However, the verification requirement will adversely impact the exercise of online expression, even if it purports to be voluntary. This is also against the core tenet of data minimisation enshrined in the GDPR and the IDPB itself that states that organisations should not collect more information than is necessary to fulfill their purpose. This obligation also contravenes the February 2018 ruling of a German Court that rendered Facebook's 'real name' policy in violation of Germany's privacy laws.[25]

Recommendations

- Clause 14 of PDPB should clarify whether the Authority or the Federal Government is sanctioned to assess the *"adequacy"* of data protection of the recipient in relation to cross-border transfers.
- A framework similar to the GDPR should also be formulated that includes in the absence of an adequacy decision, alternate conditions or other appropriate safeguards on the basis of which transfer can take place.
- Blanket exemptions in Clause 15 such as *"strategic interests"* of the State should be removed to avoid the arbitrary use of this provision.

  The requirement to localise data under clause 14 must be removed.

25. The Verge. (2018, February 12). German court says Facebook's real name policy is illegal. https://www.theverge.com/2018/2/12/17005746/facebook-real-name-policy-illegal-german-court-rules

VII. Authority

Dependence on the Government

Clause 32 of the PDPB establishes the Personal Data Protection Authority - a statutory corporate body - that shall be *an autonomous body under the administrative control of the Federal government.* However, a prerequisite for the Authority's ability to enjoy complete operational and administrative autonomy is to separate it from the Federal Government. As per clause 33, one of the functions of the Authority is to *perform such other functions as the Federal Government may, from time to time, assign to it.*

The IDPB establishes an identical body and its clause 86 empowers the Central Government to issue to the Authority *such directions as it may think necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order.*

Both the IDPB and PDPB contravene the concept of "complete independence" delineated in the GDPR. Its recital 117 stresses on the complete independence of the Authority as *an essential component of the protection of natural persons with regard to the processing of their personal data.*

This concept is also explained at length, in the landmark decisions of the CJEU where it held that the Authority should be empowered to *"perform their duties free from external influence and should not seek nor take instructions from anybody,"*[26] *and that "any influence exercised by the supervised bodies, any directions or any other external influence, whether direct or indirect"*[27] may affect the independence of the Authority's decision.

The PDPB should emulate the GDPR and these leading decisions in ensuring and safeguarding the independence of the Authority in relation to influence and supervision. However, the comparable Indian and Pakistani models of Authority vest sweeping powers in the Government by means of appointments, directions, exemptions and financial assistance. Therefore, limiting the autonomy and independence of the Authority in the exercise of its functions and duties.

Whereas, the DPA mandates the Information Commissioner's Office to act as a watchdog to oversee the enforcement of data and information legislation, and promote data rights across the UK. Instead of creating an authority under the control of the Federal Government, the PDPB should emulate the UK authority that combines the functions of the data protection commissioner mandated to protect personal data with those of the information commissioner mandated to promote access to information. The complementary nature of these two rights is that individuals have a right to request and obtain copies of information that contains their personal data (with the adjunct rights to request modification or removal of such data).

It should be considered and weighed whether the mandate to perform the duties and functions of the Authority can be entrusted to the existing Federal and Provincial Information Commissions set up under the Right of Access to Information Act 2017 instead of creating another body with excessive powers.

Financial Dependence

The PDPB, by further, allowing the Federal and Provincial Governments to give grants and loans to the Authority will threaten the very non-partisan and apolitical manner in which it should function, at all times.

26. European Commission vs. Federal Republic of Germany, 2010, C-518/07

27. European Commission v. Republic of Austria, 2012, C-614/10

Additionally, the lack of a separate, public annual budget as required by Recital 120 of the GDPR endangers Authority's independence in all three countries. Instead of an allocated budget, the UK Information Commissioner also relies on an annual grant-in-aid from the Department of Culture, Media and Sport, and annual notification fee collected from data controllers. Similarly, the Indian Authority is to be granted sums by the Central Government after due appropriation made by Parliament by law.

It is important to understand that it is not the job of the Authority to defend the interests of the Federal Government or the requestors in a partisan manner, conversely, its sole purpose is to uphold and safeguard citizens' constitutionally guaranteed rights to privacy and access to information taking into consideration the limits established by law and the public interest test.

Recommendations

- A Separate budget needs to be allocated for the Authority to ensure that its operations remain independent from the influence of the Federal and Provincial Governments, and that it can perform its functions in a non-partisan manner.

Composition of the Authority

Independence also stems from the process of selection, remuneration and removal of the Chairperson and Members of the Authority.

In order to ensure that the Authority remains technically competent and independent, its composition should not be left to the Federal Government. Clause 32 of the PDPB requires a seven-member committee to be constituted, of which one must be an ex-officio member representative of either the IT, Defence or Interior Ministry. It is impossible to ensure impartial and objective decision-making with the proposed composition of the committee. Since, the members will be paid salaries through the Personal Data Protection Fund - also to be financed by the Federal and Provincial Governments - they will be treated as government servants.

On the contrary, Schedule 12 of the DPA explicitly states that the Commissioner and their officers and staff are not to be regarded as servants or agents of the Crown. Further, it provides a more democratic mechanism for the appointment, removal and payment of salary of the Commissioner with the involvement of the Parliament.

Further, in the European Commission v. Germany case,[28] the CJEU highlighted the role that parliament should play in appointing the management of the supervisory authorities, defining the powers of these

28. European Commission v. Federal Republic of Germany 2010, C-518/07

authorities, and obligating them to report their activities to Parliament.

It is imperative that the process of nominating the members of the Authority is as open, democratic and consultative as possible. The Federal Government should not be allowed to propose nominations instead the nominations be invited from all sectors of society and the government, and be subject to the approval of the Parliament.

However, the PDPB does the opposite by empowering the Federal Government to nominate the Chairman from amongst the seven member-committee that shall also be appointed by it. The Federal Government is also authorized to increase the members of the Authority, and prescribe their qualifications and mode of appointment. It is important to note that the government is also an interested party, and if such unfettered powers are vested in it, it can conveniently manipulate and neglect the law in order to fulfil other purposes.

Regrettably, clause 42 of the IDPB contains a comparable appointment mechanism whereby the Chairperson and Members of the Authority will be appointed by the Central Government on the recommendation made by a selection committee - to be constituted of civil servants only- and paid as prescribed by the Central Government, and the chairperson will be removed by the Central Government after being given a "reasonable" hearing.

Further, the Chairman under the PDPB can be removed if they are found guilty in an inquiry conducted by the Federal Public Service Commission on directions of the Prime Minister.

It is also advisable that the Pakistani Chairman's serving term is seven years such as that of the Information Commissioner to avoid stacking the Commission with political appointees each time the government changes.

Recommendations

- Provisions that authorise the Federal Government to nominate and increase members of the Authority, nominate chairman, remove members, prescribe their qualifications, payment of salary and mode of appointment should be removed, and a more democratic and consultative process must be adopted that is subject to parliamentary approval;
- The term of the chairman under the PDPB should be seven years instead of four to avoid political appointments.

Yearly Information and Financial Reporting

While both the PDPB and the IDPB fulfil the GDPR requirement of making the supervisory body's yearly reports public, however, they fail to provide clarity on what precisely needs to be reported by the Authority in the mandatory yearly reports.

The DPA, on the other hand, has adopted Article 59 of the GDPR that requires the Information Commission to report on *its activities, which may include a list of types of infringement notified and types of measures*

taken in relation to the powers vested in it.

Whereas, clause 41of the PDPB requires the Authority to submit yearly reports *on the conduct of its affairs, including action taken for the Personal Data Protection and protection of interest of the data subjects, for that year.*

Further, the PDPB and the IDPB require the Authority to send their yearly reports to the Central and Federal Government respectively who will be responsible for placing them before the Parliament. This is in contravention with the DPA, that makes it the responsibility of the Information Commissioner to arrange for the report to be placed directly before the Parliament without any interference by the government.

To make it worse, the PDPB impugns and threatens the credibility of the Authority's reports by also empowering the Federal Government to sit on them for three months after they were first made available to them.

Another provision unique to the PDPB that gives unfettered control and access to the Federal Government is sub-clause 3 of clause 41. It requires the Authority to *supply any return, statement, estimate, statistics or other information in respect of any matter under the control of the Authority or a copy of any document in the custody of the Authority.*

Further, section 11 of the DPA Act requires the Commissioner to only send a copy to the Comptroller and Auditor General who must then examine, certify and report on that particular statement. However, as per clause 39 of the PDPB and clause 80 of the IDPB, the Authority is mandated to share all its accounts with the Comptroller and Auditor-General who shall be auditing them.

Finally, the PDPB should treat the submission of the yearly information report and the audit report separately as to avoid the unnecessary delay of three months waiting for the Auditor General to prepare his report. Both of the reports should be shared directly with the Parliament without any meddling from the Government.

Recommendations

- The PDPB should prescribe what needs to be reported in the yearly report of the Authority.
- Clause 40 should be revised to place the report directly before the Parliament without any interference by the government.
- The requirement under clause 41(3) to give unfettered control and access to the Federal Government to any return, statement, estimate, statistics or other information in respect of any matter under the control of the Authority or a copy of any document in the custody of the Authority should also be removed.
- The PDPB should treat the submission of the yearly information report and the audit report separately as to avoid the unnecessary delay and any meddling from the Government.

VIII. Compensation

Drawing from article 79 of the GDPR, clause 45 of the PDBP entitles a data subject to file a complaint with the Authority against non-compliance or unlawful processing by any data controller or processor in violation of their obligations and the rights of data subjects guaranteed under the Bill. However, the PDPB contains no specific provision that allows data subjects to be able to claim compensation for material or non-material damage suffered as provided in article 82 of the GDPR. Recital 146 demands that the concept of damage should be broadly interpreted to include compensation for distress even when it is not possible to prove financial loss.

The UK Court of Appeal expanded on this principle in its landmark decision in Lloyd v Google LLC [2019] EWCA Civ 1599,[29] where it held that damages can be awarded for the *"loss of control of private information"* even if compensation for distress is not claimed. It further added that due to the economic value of data, a person's loss of control over their data has value regardless of the fact that data is not recognised as property in English Law.[30]

Similarly, the IDPB provides an exhaustive definition of "harm" in sub-clause 20 of clause 3 that includes: *bodily or mental injury, loss, distortion or theft of identity, financial loss or loss of property, loss of reputation or humiliation, loss of employment, any discriminatory treatment, any subjection to blackmail or extortion, any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal, any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled or any observation or surveillance that is not reasonably expected by the data principal.*

This is an extremely important clause that should also be adopted in the PDPB as it would not only entitle the aggrieved data subjects to compensation for material and non-material loss (distress), but would also provide legal safeguards to gender, religious and ethnic minorities against discriminatory treatment and profiling, protection against the illicit use of CCTV cameras to monitor public spaces, unnecessary individual and indiscriminate public surveillance by both state and private companies, in addition to legal protection against restrictions on movement and speech. This clause would ensure that the rights of data subjects' remain at the heart of the PDPB and would provide clarity and establish primacy of the safeguards guaranteed under the Bill over other oppressive laws that contravene it.

Further, this would mean that data subjects would be able to move the High Courts to bring compensation claims against government and private bodies, and hold them accountable. And in the future, if any data breach occurs - similar to the disturbing leaked CCTV footage by private cinemas,[31] leaked private pictures of passengers by Punjab Safe Cities Authority,[32] or the countless leaks of the NADRA database,[33] and the Punjab Information Technology Board's mobile app,[34] or the hacking of major Pakistani Banks[35] - the aggrieved data subjects would be entitled to compensation that would cover both material and non-material damages.

29. Where a representative claim was brought on behalf of an estimated 4.4 million iPhone users Google's gathering and exploitation of browser generated information ("BGI") on Apple's Safari browser.
30. At paragraphs [46] – [47], Lloyd v Google LLC [2019] EWCA Civ 1
31. Samaa TV. (2019, September 1). Outrage after Lahore cinema releases CCTV footage of dating couples. https://www.samaa.tv/news/2019/09/outrage-after-lahore-cinema-releases-cctv-footage-of-dating-couples/
32. Dawn. (2019, January 27). Leaked Safe City images spark concern among citizens. https://www.dawn.com/news/1459963
33. Digital Rights Foundation, 2017, Lack of Accountability in NADRA, https://digitalrightsfoundation.pk/wp-content/uploads/2017/06/Updated-Infographic-01-01-1.jpg
34. Digital Rights Monitor. (2018, May 11). Is PITB clueless about Pakistan's largest data breach? https://www.digitalrightsmonitor.pk/is-pitb-clueless-about-pakistans-largest-data-breach/
35. The News. (2018, November 6). Data of major Pakistani banks hacked: FIA official. https://www.thenews.com.pk/latest/390450-data-of-major-pakistani-banks-hacked-fia-official

Although, clause 25 of the PDPB provides data subjects the *right to prevent processing likely to cause damage or distress* by writing a "data subject notice" to the concerned processor or controller requiring them to cease processing of or processing for a specified purpose or in a manner stating (i) reasons if it is causing or is likely to cause substantial damage or substantial distress to them or a relevant person, and (ii) that the damage or distress is or would be unwarranted.

However, neither "damage" nor "distress" have been defined in the PDPB, and the list of broad exceptions such as when the processing is necessary to protect the vital interests of the data subject or if consent is already given, clause 25 will not be applicable. This essentially means that the data subject's consent is irreversible and the data subject has no control over his data once they have already given consent.

Further, in order to ensure effective compensation and ease the process of filing a complaint and seeking judicial remedy, Recital 142 of the GDPR provides for the constitution of a not-for-profit body or organization mandated by the data subject that has statutory objectives which are in the public interest to do the preceding.

S.168 (3) of the DPA reiterates and allows for claims to be brought by representative bodies, and compensation to be paid to them on behalf of the data subjects if the court thinks fit.

The IDPB does not contain any such provision. However, it is imperative that the PDPB incorporates this provision and allows for a representative body that brings private complaints on behalf of data subjects especially those who are not able to assess the potential implications of the infringement of their personal data.

Clause 64 of the IDPB entitles data subjects to seek compensation directly by filing a complaint with the Adjudicating Officer whose decision can be appealed to the designated Tribunal. Whereas, the supervisory authority under the GDPR and the Information Commission under the DPA 2018 are not authorized to award compensation which can only be sought through the courts.

Article 83 of GDPR discusses the general conditions for imposing fines; when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case. However, no such safeguards are there in the PDPB.

Recommendations

- The PDPB should grant the right to compensation for material and non-material damages as provided in article 82 of the GDPR.
- It should define and interpret "damage" broadly to include compensation for distress even when it is not possible to prove financial loss.

CONCLUSION

Data protection legislation in Pakistan has been in the works for about three years at the time of writing this report (December 2020), and frequent data breaches in recent years have increased the need for a comprehensive and effective data protection law that guarantees the safety of user data. It is the constitutional right of citizens of Pakistan to have a legislative mechanism that not only protects its data subjects but works to make the digital economy secure enough to attract international investments. The PDBP, while borrowing many aspects of the "gold-standard" GDPR and the DPA, needs improvement in some crucial areas that may have a larger effect on the overall implementation of the law.

The Bill must take into consideration the excessive surveillance mechanisms that are deployed in the country by different state institutions for the sake of "national security", and must not exclude these bodies from the Act. The sensitive personal data of millions of Pakistanis is processed everyday by public bodies, putting them at high risk if the state's data protection regime does not provide safety for this data.

The PDPB should reconsider the overbroad and sweeping powers given to the Federal Government without any parliamentary oversight. Such broad powers contradict the fundamental constitutional principle of separation of powers by allowing the Federal Government to make arbitrary exemptions. Any decisions made by the Federal Government must undergo scrutiny by the Parliament before they can be implemented to ensure there is no abuse of power.

The requirement of data localization in the Bill is particularly worrisome. Keeping copies of personal data in Pakistan can prove to be damaging for the overall aim of data protection this regulation aims to achieve. Unfortunately, Pakistan has had a record of clamping down on privacy, free speech, censorship and prosecuting those who criticize the state or the establishment. Combined with the requirements of The Removal and Blocking of Unlawful Online Content Rules 2020, the localisation of data and data servers, and the storage of, the decrypted and unencrypted data of the citizens, may increase thet risk of being breached by various actors, leading to serious consequences for freedom of expression and right to privacy in the country. The State must look into other safer methods of obtaining data for counter terrorism and crime prevention, such as the Mutual Legal Assistance Treaties (MLAT) discussed earlier in the research.

In order to ensure that the PDPB is implemented effectively, the state must ensure that it prioritizes the safety of user data over surveillance and censorship, and fully incorporate the principles of lawfulness that exist in the GDPR that strikes a balance between the rights of the citizens and the duty of the state.

About MMFD:

Media Matters for Democracy (MMFD) is Pakistan's leading media development organisation, with a focus on digital democracy, Internet rights and governance, and Media and Information Literacy (MIL).

The main premise of our work is push for a truly independent, inclusive media and cyberspace, where the citizens in general, and journalists in specific, can exercise their fundamental rights and professional duties safely and without the fear of persecution or physical harm.

We also work on acceptance and integration of digital media and journalism technologies and towards creating sustainable 'media-tech' initiatives in the country.

MediaMatters forDemocracy

Policy Research & Advocacy Initiative