Pakistan Personal Data Protection Bill 2020:

Access Now inputs to Ministry of Information Technology and Telecommunications consultation

May 15, 2020

Access Now is an international non-profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence in 13 countries around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. Access Now also engages with its global community of nearly half a million users from over 185 countries, in addition to operating a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We coordinate as part of CiviCERT (Computer Incident Response Center for Civil Society) a Trusted Introducer accredited CERT and are a member of the Forum for Incident Response (FiRST). We also have special consultative status at the United Nations.[1]

At Access Now, we have been involved with the development and implementation of the EU's General Data Protection Regulation, as well as provided expertise on the formulation and enforcement of data protection and privacy legal frameworks across the world. We have published a data protection guide for lawmakers built on lessons from the EU's GDPR and global privacy frameworks that highlights do's and don'ts for comprehensive data protection legislation, which we believe will be useful towards the refinement and finalisation of the draft bill on Personal Data Protection prepared by the Government of Pakistan. In our lawmakers guide (attached to this document as annexure 1), we list the following do's and don'ts:

DO'S:

1. ENSURE TRANSPARENT, INCLUSIVE NEGOTIATIONS
2. DEFINE AND INCLUDE A LIST OF BINDING DATA PROTECTION PRINCIPLES IN THE LAW
3. INCLUDE A LIST OF BINDING USERS' RIGHTS IN THE LAW
4. DEFINE A CLEAR SCOPE OF APPLICATION
5. CREATE BINDING AND TRANSPARENT MECHANISMS FOR SECURE DATA TRANSFER TO THIRD COUNTRIES

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.

6. PROTECT DATA SECURITY AND DATA INTEGRITY
7. DEVELOP DATA BREACH PREVENTION AND NOTIFICATION MECHANISMS
8. ESTABLISH INDEPENDENT AUTHORITY AND ROBUST MECHANISMS FOR ENFORCEMENT
9. CONTINUE PROTECTING DATA PROTECTION AND PRIVACY

DON'TS:

1. DO NOT SEEK BROAD DATA PROTECTION AND PRIVACY LIMITATIONS FOR NATIONAL SECURITY
2. DO NOT AUTHORISE PROCESSING OF PERSONAL DATA BASED ON THE LEGITIMATE INTEREST OF COMPANIES WITHOUT STRICT LIMITATIONS
3. DO NOT DEVELOP A "RIGHT TO BE FORGOTTEN"
4. DO NOT AUTHORISE COMPANIES TO GATHER SENSITIVE DATA WITHOUT CONSENT
5. DO NOT FAVOUR SELF-REGULATION AND CO-REGULATION MECHANISMS

We have analysed the version of the Draft Data Protection Bill that was published in April by the Ministry of Information Technology and Telecommunications of the Government of Pakistan for public comment. We below provide our initial inputs on the current text of the bill as they relate to the parts of our lawmakers guide recommendations that we believe are most relevant. As the consultative review process continues, we hope to provide further analysis to stakeholders to help ensure the eventual enactment of a strong data protection law in Pakistan that advances privacy for all.

1. INCLUDE A LIST OF BINDING USERS' RIGHTS IN THE LAW

[Recommendation: Amend current text and insert clauses in chapter III of draft bill]

Currently, the draft bill provides several binding data protection user rights - and implementing measures for the same. However, it misses two crucially important rights that we believe are crucial for global best practice in data protection laws. Namely:

- **Right to portability**: It enables users to move certain personal data they have provided from one platform to another offering similar services. To facilitate this process, interoperability between services should be encouraged.

- **Right to explanation**: It empowers users to obtain information about the logic involved in any automatic personal data processing and the consequences of such processing. This right is crucial to bring accountability and transparency in the use of algorithms to make decisions that impact users' lives.

We recommend that these rights be added in the form of substantive clauses inserted into chapter III of the bill.

Furthermore, the bill introduces a payment requirement for the exercise of certain rights, including the right to access. For rights to be accessible and to prevent discriscrimination, the exercise of data subject rights shall not be dependent on payment and be free of charge. We recommend that the bill is amended to ensure that the exercise of all data rights are free of charge.

2. CREATE BINDING AND TRANSPARENT MECHANISMS FOR SECURE DATA TRANSFER TO THIRD COUNTRIES

<u>Recommendation</u>: Amend clauses 14 and 15 in draft bill.

The draft bill regulates the transfer of personal data, including cross border transfers. This is in line with many global practices, and we believe that secure data transfers across borders should be done so in a manner that they ensure binding protection for the rights of users and transparent mechanisms. We are currently concerned by the language proposed in clauses 14 and 15 of the bill, which would create restrictions on the processing and storage of "critical personal data" and powers to the Federal Government to choose to prohibit or exempt such restrictions. Firstly, this language uses terms which are not clearly defined in the draft bill itself. Clause 2(o) defines "Critical Personal Data" as that which is "to be classified by the Authority with the approval of the Federal Government". In effect, critical personal data will be whatever is classified as such by the Personal Data Protection Authority (PDPA) and the Federal Government, with no restrictions or guidance on such powers. Such overbroad classification powers appear to be a case of excessive legislative delegation to the executive, and will leave space open for abuse impacting the fundamental right to privacy as well as uncertainty to actors in the ICT ecosystem. Secondly, by this current text, the draft bill appears to be seeking to establish a data localisation regime in Pakistan under the garb of data protection. That is reinforced by the fact clause 15 states that the PDPA "shall also devise a mechanism for keeping a copy of personal data in Pakistan to which this act applies". We have consistently advised that data localisation is not — and should not — be a prerequisite for enforcement of data protection rules. A requirement such as this would facilitate third-party abuse of personal data and infringe on users' right to privacy, as actors would know where data is located. And mostly importantly, such proposals go against the spirit and objective of a data protection and privacy legislation and would make the final Data Protection Act of Pakistan - if enacted in the

form - inconsistent with global standards, harming its possibilities of securing data protection adequacy status with other jurisdictions.

3. DEVELOP DATA BREACH PREVENTION AND NOTIFICATION MECHANISMS

<u>Recommendation</u>: Amend clause 13 in draft bill.

It has been our recommendation based on our experience with data protection law making that notification to users should be a requirement for any data breach of personal data, which includes any personal data submitted by the data subject or acquired by the data processor (such as photos). Notification should be timely, easy to understand, and comprehensive, and remediation options should be clearly indicated and accessible. Leaving too much discretion to organisations can result in a law that falls short of empowering users to take control of their information. Organisations suffering a data breach have an obvious economic interest in downplaying the risks associated with a breach and not notifying users, which could result in unaddressed data protection and security violations. Data subjects shall be notified when accounts or personal information are compromised so that they can take all necessary steps to prevent further abuse of these data which may include theft, or fraud. We encourage lawmakers around the world to avoid those shortcomings and develop unambiguous data breach prevention and notification mechanisms.

We are concerned that the current text of clause 13 of the draft bill pertaining to data breach notification falls short of this standard. It currently only mandates that a data breach has to be reported expeditiously to the PDPA. It does not require that PDPA to help facilitate notification to data subjects, nor does it clearly state that data controllers and processors are legally permitted - and obliged - to inform affected users expeditiously. This should be clearly included in the law, by suitably amending this clause.

4. ESTABLISH INDEPENDENT AUTHORITY AND ROBUST MECHANISMS FOR ENFORCEMENT

<u>Recommendation</u>: Review and amend chapter VI of draft bill, including clauses 32, 34, 38, 39.

The importance of a well designed, independent regulatory authority in a data protection law cannot be overstated. In our global lawmaker recommendations, we have emphasised that even the best data protection law in the world would be close to meaningless without an authority having the powers and resources to monitor implementation, conduct investigations, and sanction entities in case of (repeated, neglected, or willful) data protection violations.

We are concerned that the current text of the draft bill would result in the creation of a PDPA that falls short of having an independent data protection authority. Currently chapter VI of the bill, particularly clauses 32, 34, 38 would result in a PDPA that is not sufficiently independent of the executive branch. It proposes that several representatives of existing Federal Government ministries will sit *ex-officio* on the PDPA and will take part in the proceedings and decision-making of the PDPA. This is also further concerning given that the quorum of the PDPA is fixed at three members attending, which could lead to situations where the executive branch ex-officio members are able to effectively run the affairs of the PDPA without the independent, full-time members.

Additionally, the appointment process for the members is not sufficiently developed to ensure that independent, talented experts are appointed to the PDPA. The text only states that the Federal Government shall appoint them, with no indication of an independent appointment process, cross stakeholder input, or legislative oversight or involvement. The text in fact indicates that the Federal Government also has the power to change the appointment process at any time, without any requirement of approval, review, or legislative amendment by the Parliament of Pakistan. This executive branch influence is exacerbated by the fact that the draft bill provides the decision-making power and control over wages of the members of the PDPA to the Federal Government. Even if the members and staff seek to ensure its independence, their efforts can be legally overridden by the power granted under clause 38 to the Federal Government to issue binding policy directives to the PDPA.

Independence of the PDPA and its government body is crucial, especially given that often it will be government agencies and government service related data transactions that may end up before it for investigation and adjudication.

International cooperation by the PDPA - crucial in this world of the global internet and cross-border data flows - is also made subject to pre-approval by the Federal Government; a requirement of coordination or advice of the Federal Government may be more appropriate and allow for more efficient, faster global cooperation for sharing best practices, relevant information, and effective enforcement.

5. **DEFINE A CLEAR SCOPE OF APPLICATION;**
   and
   DO NOT SEEK BROAD DATA PROTECTION AND PRIVACY LIMITATIONS FOR NATIONAL SECURITY

   <u>Recommendation</u>: Review and amend clauses 24, 30(2) in draft bill.

In our lawmakers guide, we note that any national security exceptions in a data protection law must be prevented and limited to clearly defined, necessary, and proportionate measures that include judicial oversight and accessible remedy mechanisms. Legislation should not give

governments and public entities the capacity to shield themselves from the obligation to protect users' right to data protection. In fact, countries have a security interest in safeguarding personal data held by government agencies.

Furthermore, obligations under data protection law should clearly apply to both the private and public sector. Public authorities are increasingly collecting individuals' information, getting access to private-sector databases, or otherwise building large databases of personal data. This processing shall be subject to clear obligations for the protection of individuals' personal information, the same way that processing by private entities is regulated

Provisions in the draft bill provide exceptions to other data protection mandates to law enforcement and security agencies, particularly by the use of the broad term of data relating to "the prevention or detection of crime or for the purpose of investigations", "the apprehension or prosecution of offenders", or "the assessment or collection of any tax or duty or any other imposition of a similar nature". It would be better to state the specific laws under which such activities would be regarded as legitimate exceptions, and ensure that those meet international human rights law standards, particularly those of necessity and proportionality.

Additionally, the law allows for a wide power to restrict processing of data on security grounds that the Federal Government totally controls, stating that "the processing of personal data in the interests of the security of the State provided that the processing of personal data shall not be permitted unless it is authorized pursuant to an express authorization by the Federal Government and in accordance with the procedure to be laid down by the Federal Government in this regard". This may be an overbroad power, particularly since the establishment of the procedure to be followed by the Federal Government is delegated to the Federal Government itself to establish, with no legislative oversight or other checks.

6. **ADDITIONAL AREA OF CONCERN**: **Avoid creating a data protection "licensing framework"**

   <u>Recommendation</u>: Amend clause 34(f) to omit any reference to powers for a licensing framework.

Data protection laws are meant to provide clear, enforceable data protection rights to users, set in place principles to govern the consent, processing, use, and transfer of data, and ensure effective enforcement and oversight of the activities of data controllers and processors. The regulatory focus flows from activities that touch upon personal data. They do not require licensing, in the manner that might be seen in areas dealing with natural resources or relevant policy needs that justify such additional control. A data protection "licensing" framework would be overbroad, not workable, and may chill the easy development and use of ICT services by users that are often crucial for the exercise of their human rights in our digital age.

Conclusion

We hope that the Ministry of Information Technology and Telecommunications considers our inputs and the concerns of all stakeholders in further reviewing and improving the Draft Data Protection Bill. Inputs from this current consultation would be best used in providing an updated draft of the bill, which is made available for further review and inputs prior to its introduction for consideration and passage in the Parliament. As we have noted in our lawmakers guide and witnessed in several legislative processes on data protection laws globally, it is crucial to focus on ensuring "**transparency and inclusive negotiations**" in order to have a well drafted law that is well accepted and adopted by all stakeholders.

For any queries, please reach out to our Asia Pacific Policy Team via Lucie Krahulcova, Asia Pacific Policy Analyst (lucie@accessnow.org). This document has been prepared by our Asia Pacific Policy Team with the assistance of Estelle Massé, Global Data Protection Lead (estelle@accessnow.org).