Personal Data Protection Bill, 2018

Civil Society Submission to the Ministry of Information Technology and Telecommunications

August, 2018

A joint submission by Digital Rights Foundation and Privacy International

About us

This submission is made by the Digital Rights Foundation (DRF) and Privacy International (PI).

The **Digital Rights Foundation** (DRF), founded in 2012, is a research-oriented and advocacy not-for profit organization working on issues of online freedom of expression, the right to privacy and online violence. DRF aims to make the internet a safe and accessible space for all. www.digitalrightsfoundation.pk

Privacy International was founded in 1990. It is the leading charity promoting the right to privacy across the world. Working internationally through an International Network of partners, Privacy International works, within its range of programmes, investigates how our personal data is generated and exploited and advocates for legal, policy and technological safeguards. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.
https://privacyinternational.org/

Contacts

Nighat Dad
Executive Director, Digital Rights Foundation

nighat@digitalrightsfoundation.pk

Shmyla Khan
Project Manager, Digital Rights Foundation
shmyla@digitalrightsfoundation.pk

Ailidh Callander
Legal Officer, Privacy International
ailidh@privacyinternational.org

Alexandrine Pirlot de Corbion
Programme Lead, Privacy International
alex@privacyinternational.org

Overview

Privacy is a fundamental human right. Protecting privacy in the modern era is essential to effective and good democratic governance. This is why data protection laws exist in over 120 countries worldwide,[1] and instruments have been introduced by international and regional institutions such as the African Union,[2] the OECD,[3] Council of Europe,[4] and ECOWAS.[5]

In Pakistan the right to privacy is guaranteed under Article 14(1) of the Constitution: "[t]he dignity of man and, subject to law, the privacy of home, shall be inviolable." This Article vests in its citizens the fundamental right to privacy and it has been interpreted to extend to digital communications as well.[6]

Data protection is about safeguarding our fundamental right to privacy by regulating the processing of personal data: providing the individual with rights over their data, and setting up systems of accountability and clear obligations for those who control or undertake the processing of the data.

We welcome the effort by the Ministry of Information Technology and Telecommunications (henceforth referred to as "**Ministry**") Government of Pakistan to regulate the processing of personal data in Pakistan. We also appreciate the opportunity to inform this consultative process and we look forward to engaging in the next steps. We hope that an inclusive, transparent and well-defined consultative process is laid out by the in-coming government that takes into account the civil society, digital rights organisations and the public at large.

While comprehensive in some aspects, the "Personal Data Protection Bill" (henceforth referred as "**Bill**") proposed by the Ministry has a number of significant shortcomings. We recommend that to effectively protect privacy and meet international standards in protecting personal data, full consideration be given to the areas of concern and improvements outlined below under each Part of the Bill:

---

[1] See Graham Greenleaf, Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey (2017) 145 Privacy Laws & Business International Report, 10-13, UNSW Law Research Paper No. 45available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035

[2] See the African Union Convention on Cyber security and Data Protection, 2014, available at http://pages.au.int/infosoc/cybersecurity

[3] 3See the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, updated in 2013, available at http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[4] See the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, 1981, available at http://conventions.coe.int/Treaty/en/Treaties/html/108.htm

[5] See the Supplementary Act on personal data protection within ECOWAS, February 2010, at http://www.ecowas.int/publications/en/actes_add_telecoms/SIGNED-Personal_Data.pdf

[6] Benazir's Case, PLD 1998 SCMR 388; Taufiq Bajwa vs CDGK (2010 YLR 2165); M.D.Tahir v. State Bank, 2004 CLC 1680.

1. **To include public bodies and government-held personal data**: within the ambit of the Act by not restricting it to commercial transactions;
2. **Expanding the definition of "personal data"**: under section 2(h) to include all personal data held by both private and public bodies without the caveat of "commercial transactions" attached to it;
3. **Define the scope of the Act clearly**: to ensure that the rights of data subjects are protected regardless of where their data is processed or held;
4. **Definition of Consent**: Given that consent of the data subject is the major principle guiding data collection, it is important that section 2 of the Bill define consent and that the definition ensure that consent is explicit, free, informed, proactive and specific;
5. **The definition of "sensitive personal data":** needs to be expanded to include biometric and genetic personal data;
6. **Safeguards against mass surveillance**: Data processing by law enforcement agencies and investigative and intelligence bodies needs to be addressed by the Bill. These authorities should be subject to the standards of necessity and proportionality enshrined in international human rights law;
7. **International data sharing**: needs to be addressed by this Bill and higher standards should be in place to govern such transfer;
8. **Limit broad powers given to the Federal Government to make exemptions**: Exemptions to the Act should be limited and we recommend that the Bill be amended to limit broad powers awarded to the Federal Government, and to ensure that any deviations from the Act be subject to an open, inclusive and transparent legislative process.

Chapter 1 Preliminary

1. Short title and commencement

Section 1 (1) notes the law would be called the "Personal Data Protection, 2017". The data given to the law should be the year it is voted and adopted in.

The territorial scope of application provided for in section 1 (2), which states the Act would "*extend to the whole of Pakistan*", does not provide sufficient clarity on the scope of the law given that certain regions that fall within the country's boundaries are considered beyond the law's reach (e.g FATA). This must be reviewed to ensure the applicability of the law is clear and unambiguous.

Legislators have an obligation to protect the rights of those in their jurisdiction, including the right to privacy and data protection. Therefore, in order that individuals are not deprived of the protections they are entitled to, data protection frameworks should be clear as to how the law applies, to whom and how it protects individuals in each of these scenarios:

- The data controller/data processor is established in the relevant jurisdiction, even if processing takes place elsewhere;

- The controller or processor is not established within that jurisdiction, but is processing personal data of an individual in that jurisdiction; and
- The data is transferred to a third party outside that jurisdiction.

2. Definitions

'data subject'
It is posited that any "individual" can be a data subject, however it is unclear whether this includes natural persons or legal persons (such as corporate entities). Clarity the definition of the data subject will also determine the *locus standi* of aggrieved parties under the Act. It is recommended that the definition of individual should be restricted to natural persons.

'personal data'
The definition of personal data is limited. It is not explicit as to what personal data is and indirect identification is limited to data in possession of data controllers. This limitation should be removed.

Furthermore, from the wording of the current definition of 'personal data' provided, it seems that the scope of the definition, and as a result the Act, would be limited to personal data in respect of 'commercial transactions' only. Limiting the definition of personal data to exclusively commercial transactions excludes public bodies and all data not directly related to commerce. This is extremely limiting, especially given the huge amount of data electronically held by the government—the Bill should apply to all personal data.

The narrow definition of personal data also undermines the underlying principles of data protection as a fundamental right, stemming from Article 14, rather than a commercial protection accorded to parties in a commercial transactions. The Bill, as it currently stands, means that persons living in Pakistan/residents of Pakistan only have the right to privacy in their role as customers and not as persons living in Pakistan/residents of Pakistan.

Without these changes this definition effectively means that in practice the Act would only cover a limited amount of personal data and the protections contained therein would be severely restricted.

'Third party'
Subsection 2 (j) refers to "data user" in the definition of "third party". Clarification is necessary as to who a 'data user' (section 2(j)(iii)) is and how this differs to data controller. A"relevant person" is also not defined and it is open to interpretation whether this is a legal representative, guardian or blood relative.

Furthermore the exception included under subsection 2(j)(v) is counter-intuitive since it excludes anyone that the "data user" has authorized, essentially creating a loophole for data controllers and processors who wish to share data with third parties, free of the restrictions placed under this legislation.

'Sensitive personal data'
The definition for 'sensitive personal data' must also include biometric and genetic data.

Some consideration should be given as to whether there are any other categories specific to the Pakistani context that should be added. Considering the local context and realities are an important step in ensuring that relevant safeguards are provided for in legislation.

It is also important that higher protections extend to data which *reveals* sensitive personal data, through profiling and the use of proxy information (for example, using someone's purchase history to infer a health condition), it is possible for those processing data to infer, derive and predict sensitive personal data without actually having been explicitly provided with the sensitive personal data. Gender identity and sexual history should explicitly be included within the ambit of the definition.

'Consent'
Consent is not defined in the Bill, this is problematic as several clauses refer to the term throughout the Bill.

The definition of consent should reflect individual's free and informed choice. Consent must be freely given, specific, informed, and unambiguous, and can be a written statement, including by electronic means. It should be explicit and require an active process for the individual, rather than a passive opt-out process: as such, it requires positive affirmative action. The entity processing the data must be able to demonstrate they sought and received consent. Currently the Bill requires explicit consent only for sensitive personal data, rather than all personal data, but even then explicit consent is not properly defined. We contend that explicit consent should be required for both personal and sensitive personal data.

3. Scope and applicability

Echoing concerns noted above in relations to the definition of 'personal data', the wording of the scope of the law provided for in subsection 3 (1) limits to the application of the law to personal data processed in respect to 'commercial transactions'.

Subsection 3(2) of the proposed Bill offers some clarity on the question of territorial jurisdiction raised in subsection 1(2). The Bill bounds all entities and individuals who are established within the territories of Pakistan, and thus will not protect data of Pakistani citizens processed and stored abroad.

The blanket exemption provided for government entities in subsection 3 (5) (c) must be revised. Data protection legislation should apply to both public and private institutions. It is unacceptable practice that public institutions (including law enforcement and intelligence agencies) be completely exempt from having obligations to protect the personal data of data subjects, or for exemptions to be excessively wide or vague. In Pakistan, the largest repository of personal data is held by the government, i.e. the National Database & Registration Authority, and this exemption places citizen data outside the protections of the proposed Bill. The law should specifically provide for the development and inclusion of standards applicable to the protection of personal data which is collected and processed for the purposes of public safety, defence, state security and investigation or prevention of criminal offences.

These provisions should, at a minimum, identify the public bodies mandated to collect and process personal data, fully respect and protect the right to privacy, and comply with the principles of legality, necessity and proportionality identified by international human rights experts, all under the supervision of an external body.

This is the first instance in which the term "public interest" has been employed, and it is used throughout the text of the Bill. It is important to define public interest within the context of personal data protection as it has been widely interpreted within Pakistan legal jurisprudence; however in the context of data protection it must encompass various, and often conflicting, ideas of privacy, personal dignity, freedom of expression and right to information. Under subsection 5(b)(ii) it is posited that personal data can be processed for "journalistic, artistic or literary purposes" if it serves the wider public interest, however there is very little clarity on how the balance between the right to know and the right to privacy.

Chapter II Processing of Personal Data and Obligations of Data Controller.

5. General requirements for personal data processing

The exceptions included under section 5(2) provide wide loopholes for data controllers to bypass the consent requirements in subsection 5(1)(a). Given that the consent of the data user is the bedrock of this Bill, exemptions should be narrowly worded and limited their scope. Subsection (2)(a), for instance, allows for opting out of the consent requirement through contractual terms and conditions. This opens the possibility of floodgates that can result in companies and entities drawing up complex contracts that discard consent by justifying it as a contractual obligation. While fulfilment of contractual obligations should be allowed for, nevertheless a caveat for reasonable contractual terms and conditions should be added.

Similarly, section 5(1)(e) exception does not include requirements for a specific court mandated order, rather the more vague purpose "for the administration of justice".

6. Notice to the data subject

We welcome the inclusion of this obligation, but it must be revised in order to require that the data controller must also notify the data subject about:

- the legal basis for processing of their data,
- the envisaged time limits for retention, and so deletion, of the different categories of data,
- the existence of profiling, including the legal basis, the significance and the envisaged consequence of such processing for the data subject, and
- the existence of automated decision-making and at the very least meaningful information about the logic involved, the significance and the envisaged consequence of such processing for the data subject.

Furthermore, it is encouraging that the Bill speaks of choices to be provided to the data subject regarding the collection of their data. It is important that subsection 6(1)(f) also require data controllers to provide opt-ins for any data collection that is not directly necessary and essential to the service being provided. All extraneous data, not essential to the service being provided or legally defined purpose, should be subject to the option of opt-ins so that consent can be easily withdrawn by the data subject.

The time limit for notice (subsection 6(2)(1)) should be given as soon as is reasonably possible as opposed to "practicable", making it subject to an objective standard rather than the capacity of the data controller.

7. Non-disclosure of personal data

This clause refers to "consent" but as noted above the Bill fails to provide a definition for consent.

Consent is a core principle of data protection which allows the data subject to be in control of when their personal data is processed: it relates to the exercise of fundamental rights of autonomy and self-determination. See above for further details on the definition of consent.

8. Security requirement

The security requirements outlined in the section need to be subject to baseline and minimum requirements regardless of what is practicable. Furthermore, in the event of a breach of security and data, there should be a requirement for the data controller and processor to immediately, or within at least a specific time period, i.e. 72 hours, inform the data subject in order to ensure transparency and maintain the principle of notice to the data subject.

9. Data retention requirements

The retention of data is made contingent on the fulfilment of purpose, however the duration of the purpose should be known to the data subject. Furthermore it should be explicitly known by the data subject that this data might be retained even after termination of service.

The Act should make clear how the obligation provided for in section 9 interacts with provisions in other legislation which require the retention of personal data. This is particularly relevant given the 1-year retention requirement for service providers under Section 29 of the Prevention of Electronic Crimes Act 2016 which we have previously argued is disproportionate and unnecessary for the aim pursued.[7]

Chapter III Rights of Data Subjects

12. Right of access to personal data

Section 12 (2) notes that a data subject must make a "*payment of prescribed fee*" if they submit a request to access their personal data which has been processed. Individuals should bear no cost in exercising this right. Furthermore, the requirement to furnish a data request in writing can have the effect of excluding those who are not able to file a written request due to illiteracy, lack of familiarity with procedure or disability. The requirement needs to be supplemented with an obligation placed on the data controller to provide assistance to those who wish to file a request but cannot file formal complaint due to certain limitations.

---

[7] "Privacy International's Comments on the draft Prevention of Electronic Crimes Act, 2015 (Pakistan)", April 2015, http://digitalrightsfoundation.pk/wp-content/uploads/2015/04/Prevention-of-Electronic-Crimes-Bill-2015-Legal-Analysis_0.pdf.

We would also like to flag that section 12(4) renders the enjoyment of the right to access tedious and cumbersome for a data subject. The ability of a data subject to comply with this process would be challenging as the data subject may not be aware that the data controller has separate entries in respect of the personal data it holds about them. Finally, in the current form of the Bill which requires a data subject to pay to request their personal data according to clause 12 (2), the treatment of each request separately would render the process very onerous and this would likely deter data subjects from exercising their right to access their personal data.

14. Circumstances where data controller may refuse to comply with data access request

Section 14 (1) (a)(ii) refers to a "*relevant person*" but this term is not defined anywhere in the law. Clarity is sought on this term and this clause.

We would also present our concerns with section 14(b) and (c) as it could be open to abuse and put the burden on data subject. Further clarity must be provided with regards to each of these instances to ensure they are used in limited and prescribed circumstances. Furthermore, subsection 14(1)(g) should be limited to trade secrets, or objectively confidential information with regards to the business of the controller.

20. Extent of disclosure of personal data

Section 20 (d) allows the data controller to disclose the data of an individual for *"any purpose*" other than the purpose for which they collected the data if they *"acted in the reasonable belief that he would have had the consent of the data subject if the data subject had known of the disclosing of the personal data and the circumstances of such disclosure."* This provision is too broad, and raises questions such as on the basis of what information would the data controller be able to make such a claim? Furthermore, the test of 'reasonable' belief is too low, rather a more objective standard needs to be applied in order to safeguard the interests of the data subject.

Section 20 (e) allows the data controller to disclose the data of an individual for *"any purpose*" other than the purpose for which they collected the data if *"the disclosure was justified as being in the public interest in circumstances as determined by the Commission."* This provision is too broad. The determination of 'public interest' must be defined by the Act, and the circumstances prescribed on the face of the legislation, not merely rely on guidance from the Commission.

22. Right of foreign data subjects

Section 22 of the Bill lacks clarity as it fails to clearly define what the rights of foreign data subjects are. A plain reading of the section implies that local data controllers are subject to foreign laws, while the same rights are not extended to Pakistani citizens whose data is stored abroad. We put forward the position that the protection of an individual's data should not depend on their immigration status.

22A. Right to erasure

Section 22A must specify clearly what *"undue delay"* is by providing a specific timeframe.

Chapter IV Processing of sensitive personal data

23. Processing of sensitive personal data

The Bill creates two tiers of personal data: a) personal data and b) sensitive personal data. Sensitive personal data personal data can only be collected in circumstances where both explicit consent is given by the data subject and that the processing is necessary. As stated earlier, the definition of sensitive personal data should be expanded to include biometric and genetic data. Furthermore, the criteria for "necessary" laid down in section 23(1)(b) is at times vague. Subsection 23(1)(b)(vi) casts a wide net by allowing sensitive personal data to be processed for "obtaining legal advice" and does not track onto legal practice and custom within Pakistan. Since legal advice can happen at any stage of a legal proceeding, it is not overseen by the court or a judicial officer. We believe that processing of sensitive personal data cannot be deemed necessary for the mere purpose of obtaining legal advice. Additionally, subsection 23(1)(b)(viii) includes within the ambit of necessary as sensitive personal data required for "administration of justice". This subject should be qualified with the requirement of a court order with reference of a particular case.

Most importantly, section 23(1)(b)(x) gives too wide a discretion to the Commission. Conditions for processing sensitive personal data must be limited and be clear and provided for by law.

We also contend that section 23(c) should be interpreted narrowly. Careful consideration should be taken where such a condition is proposed as it raises the following questions: what does 'made public' mean, how can it be verified that it was made public by an individual. Importantly, even if an individual has made data public, this does not mean that their data can be used by anyone for any purpose.

We also urge the Ministry and law makers to revise the definition of "healthcare professional" to be narrowed to include only those practitioners qualified to handle sensitive personal data.

Chapter V EXEMPTIONS

25. Exemption

We would suggest including non-governmental organisations working for the public interest within research exemption provided for in this section. Furthermore refining the language regarding investigative and legal proceedings, subsection 25 (2)(a)(ii) in particular, by making it subject to judicial oversight and a reasonability test.

26. Power to make further exemptions

Subsection 26 (1) provides very wide delegated powers to the Federal Government *"to exempt the application of any provision of this Act to any data controller or class of data controller",* thus bypassing effective parliamentary scrutiny. We recommend that the Bill is amended to

limit such broad powers awarded to the Federal Government, and to ensure that any deviations from the Act be subject to an open, inclusive and transparent legislative process.

Chapter VI The Commission

27. Commission for Personal Data Protection

We endorse the inclusion of experts in the field of technology and digital rights in the commission along with a member of the judiciary, however since the Commission has judicial powers all members should either be given training on the law relating to technologies and privacy in particular, and the law on legal procedure in general; or the Commission should also contain an advisory board of lawyers and academics who are experts in the field. A common criticism of non-judicial bodies performing judicial functions is a lack of understanding of the law, thus we posit the Act should anticipate these issues.

29. Powers of the Commission

Section 29 awards the Commission wide discretion, it must be reviewed to ensure that its powers do not permit it to bypass effective parliamentary scrutiny.

Subsection 29 (b) mentions a payment schedule for the filing of complaints. There should be no costs for data subjects to file a complaint with the Commission.

Chapter VII Complaint and Offences

36. Complaint

This section should provide for collective redress. The information and power imbalance between individuals and those controlling their personal data is growing and collective complaints would ensure corrective action by organisations processing personal data, which would benefit all those affected. Provision should therefore be made in the process to allow individuals to be represented by qualified representatives and for certain qualified bodies, such as non-profit groups working in the field of data protection, to make complaints and seek remedies. The Bill does not posit a definition of “aggrieved person”. It is not clear from the section whether the aggrieved person is exclusively the data subject or under what circumstances can others file a complaint on behalf of the data subject.

Furthermore, as noted in relation to Clause 29(b), there should be no costs associated with filing a complaint to the Commission. Therefore, Clause 36(3) must be removed.

Submitting a complaint using the ‘prescribed’ sample form should be optional.

37. Prosecution

The threshold in clause 37(2)(c) to demonstrate that *"the complainant is likely to suffer irreparable loss"* is too high. This threshold must be revised to not be to the detriment of the complainant.

We are also concerned with the role of the police in investigating the complaint. We would strongly suggest that instead of involving law enforcement, the Commission be given enhanced investigatory and enforcement powers. The Commission must also be provided with the resources necessary to carry out such investigations and enforcement action.

We would also like to note that the while the Bill empowers the Commission to impose fines, it does not grant it the power to provide compensation to complainants who have suffered harm as a result of a data breach. We urge the Ministry to empower the Commission to direct monetary compensation to be paid in proportion to the financial, technological, social and physiological loss suffered by the complainant.

Chapter VIII Miscellaneous

40. Temporary provisions

We would challenge the need for a grace period for data controllers and processors to adopt the necessary security measures which is currently provided for in section 1(3).

41. Power to make rules

We would also challenge the extensive delegated powers awarded by section 41 to the Federal Government to make rules. Any changes and/or evolutions in the obligations and safeguards provided in this law must be subject to an open, inclusive and transparent legislative process.