A Guide to Drafting Privacy Policy under the Personal Data Protection Bill, 2019

August 26, 2021

By **Shweta Reddy**

Reviewed by **Pallavi Bedi and Amber Sinha**

The Centre for Internet and Society, India

https://cis-india.org

Template designed by Saumyaa Naidu

A Guide to Personal Data Protection Bill, 2019 Compliance - Privacy Policy

The Personal Data Protection Bill, 2019, (PDP Bill) which is currently being deliberated by the Joint Parliamentary Committee, is likely to be tabled in the Parliament during the winter session of 2021. The Bill in its current form, doesn't have explicit transitory provisions i.e. a defined timeline for the enforcement of the provisions of the Bill post its notification as an enforceable legislation. Since the necessary subject matter expertise may be limited on short notice and out of budget for certain companies, we intend to release a series of guidance documents that will attempt to simplify the operational requirements of the legislation.

Certain news reports had earlier suggested that the Joint Parliamentary Committee reviewing the Bill has proposed 89 new amendments and a new clause[1]. The nature and content of these amendments so far remain unclear. However, we intend to start the series by addressing some frequently asked questions around meeting the requirements of publishing a privacy notice and shall make the relevant changes post notification of the new Bill. The solutions provided in this guidance document are mostly based on international best practices and any changes in the solutions based on Indian guidelines and the revised PDP Bill will be redlined in the future.

The frequently asked questions and other specific examples on complying with the requirements of publishing a privacy policy have been compiled based on informal discussions with stakeholders, unsolicited queries from smaller organizations and publicly available details from conferences on the impact of the Bill. We intend to conduct extensive empirical analysis of additional queries or difficulties faced by smaller organizations towards achieving compliance post the notification of the new Bill. Regardless, any smaller organizations(NGOs, start-ups etc.) interested in discussing compliance related queries can get in touch with us.

Disclaimer: This document isn't intended to substitute legal advice. The document merely outlines a few queries and procedures to draft a privacy policy.

Existing research on state of privacy policies in India

[1]https://economictimes.indiatimes.com/news/politics-and-nation/parliamentary-panel-examining-personal-data-protection-bill-recommends-89-changes/articleshow/80138488.cms

The requirement of publishing a privacy notice exists under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (SPDI rules). Multiple studies have been conducted in India to determine the level of compliance of privacy policies with the existing requirements. Some of the key deficiencies are as follows:

Placement of privacy policies

The SPDI rules are lax regarding the placement of the privacy policies i.e. the Rules require the policies to be published on the website without any reference to the data collection points. However, existing research has indicated that policies are usually hyperlinked at the bottom of the page wherein the text of the hyperlink is smaller than the rest of the page[2] or deeply embedded in the website[3] which can make it conspicuous in certain cases.

Lack of specificity

Organisations didn't explicitly specify the sensitive personal data categories that were being collected.[4] The terminology used was also vague as phrases such as “may collect”, “information such as” were used which does not provide the necessary level of specificity to the individual providing data.[5]

Most of the policies used vague and ambiguous terms to describe the purpose of processing. The vague phrasing can permit extensive usage of data[6]. For example in the statement, “we collect your personal data to improve our services” : there is no clarity on the type of services in question and what sort of actions will be taken by the organisation to improve them.

The privacy policies do not have details regarding the data retention policies[7] i.e. for how long is the data usually stored and what happens to the data after such a period and if the individual withdrew consent to the processing of personal data.

Details of data sharing with third parties

The privacy policies do not provide a very specific list of the third parties that have access to the personal data being collected by the data fiduciary. There is usually only an illustrative list of third parties[8] or some details on information sharing with related companies through the use of complicated legalese[9].

---

[2] https://cis-india.org/internet-governance/files/Hewlett%20A%20study%20of%20FinTech%20companies%20and%20their%20privacy%20policies.pdf

[3] https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf

[4] https://cis-india.org/internet-governance/files/Hewlett%20A%20study%20of%20FinTech%20companies%20and%20their%20privacy%20policies.pdf

[5] https://cis-india.org/internet-governance/files/Hewlett%20A%20study%20of%20FinTech%20companies%20and%20their%20privacy%20policies.pdf

[6] https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf

[7] https://cis-india.org/internet-governance/files/Hewlett%20A%20study%20of%20FinTech%20companies%20and%20their%20privacy%20policies.pdf

[8] https://cis-india.org/internet-governance/files/Hewlett%20A%20study%20of%20FinTech%20companies%20and%20their%20privacy%20policies.pdf

[9] https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf

Absence of grievance redressal mechanisms

Very few organisations specified the contact details of the grievance office with respect to addressing privacy complaints, and the organisations that do specify the details omit information related to the exact authority and responsibility the person had.[10] In some cases if the organisation has mentioned a grievance officer regarding the actual services being provided, it can get confusing to verify if the same grievance officer can be approached for privacy related complaints. [11]

Option to opt out

Even in cases where the processing is based on consent, the option to opt out is limited and is provided only in relation to receiving correspondences from the data fiduciary.[12]

Additional requirements in PDP, 2019

In addition to addressing these key deficiencies organizations will also have to take into consideration the additional requirements proposed in the current version of the Bill to draft their privacy policies. The additional requirements are as follows:

Timing of privacy policy

The PDP Bill has relatively explicit obligations pertaining to the placement of the privacy policies. The Bill requires the policy to be displayed at the time of collection if collected directly from the data principal and as soon as reasonably possible if collected from a different source[13]. Such specificity is absent in the SPDI rules which only requires the privacy policy to be published on the website.[14]

Personal data collected from different source

The Bill requires organizations to provide data principals with a privacy notice even in cases where the data has not been directly obtained from them.[15] Such a requirement is absent from the existing SPDI rules and will require entities to be aware about the data being accessed and examine an efficient method to provide the privacy notice to the data principal.

Legal basis of processing

Lawful processing of personal data under the SPDI rules usually relied on the consent of the individual[16]. The SPDI rules didn't have the wide range of acceptable legal basis for processing personal data that is currently allowed by the PDP Bill. [17] The proposed framework sets a high standard for consent to be a valid ground of processing. It is essential that entities that are relying on consent assess whether the consent being provided by the individuals is free, informed, specific and capable of being withdrawn[18]. In the absence of

---

[10] https://cis-india.org/internet-governance/files/Hewlett%20A%20study%20of%20FinTech%20companies%20and%20their%20privacy%20policies.pdf

[11] https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf

[12] https://cis-india.org/internet-governance/files/Hewlett%20A%20study%20of%20FinTech%20companies%20and%20their%20privacy%20policies.pdf

[13] Section 7

[14] Rule 4

[15] S.7(1)(f)

[16] Rule 5

[17] S.11, 12, 13, 14

[18] S. 11

complying with the required threshold, entities will need to examine if their purpose of processing is satisfied by the other lawful grounds identified in the legislation. The details of the legal basis identified will need to be stated in the privacy policy.

Multiple languages

The PDP Bill requires entities to provide the privacy notice in multiple languages where necessary and practical[19]. The implementation of this requirement in a diverse country such as India will have to be deliberated by entities.

Frequently Asked Questions

1. **What's the difference between a data fiduciary and a data processor?**
   If an organization is determining the purpose and means of processing the personal data being collected, then it is a data fiduciary for the purposes of the PDP Bill.[20] For example: Company A is offering the service of notifying individuals with the details of the statewide and nationwide covid-19 statistics. To provide this service, Company A requires the contact details of individuals who would like to opt in for the service. In this case Company A is a data fiduciary as they are determining the categories of personal data that needs to be collected to provide a particular service.
   If an organisation has been contracted to provide services on behalf of the data fiduciary,[21] It is a data processor for the purposes of the PDP Bill.
   For example: In the above mentioned example, if Company A decided to use the services of a third party (Company B) on their website to collect and send notifications, Company B would be the data processor for the purposes of the Act.

2. **Do both data fiduciaries and processors need to draft and publish a privacy policy?**
   The obligation of drafting and publishing a privacy policy is only on the data fiduciary. However, a data processor might be required to draft and publish such a policy based on the terms of the data processing agreement between the data fiduciary and data processor.

3. **Is the office email address of an individual personal data?**
   Yes it is. Any information that can personally identify the individual is personal data.

4. **What is the difference between a privacy policy and terms and conditions?**
   Privacy policies specify the obligations of the organizations collecting and processing personal data to the individual. Organisations are required to adhere to the privacy policies while collecting and processing personal data. Terms and conditions are the guidelines that the users of the service of the organisation are required to adhere to.

5. **Does an organization that is using third parties to enable functionality on the website include details about the data being collected by such third parties?**
   Yes. The data fiduciary that has employed the services of the third parties will need to include the data that is being collected by such third parties in their privacy policy.

[19] S. 7(2)
[20] S. 2(13)
[21] S. 2(15)

6. **Is there a template that organizations can follow?**
   The data processing operations of organizations will vary extensively. Total reliance on a template may not accurately portray an organization's practices thereby raising the risk of a potential legal action. Certain templates can be relied on purely for their form and structure but not their content.

7. **Is a privacy policy required if :**

   a) **the organization is a small non-commercial, non - ecommerce, India based site?**

      An organization's non commercial and non ecommerce status doesn't have a bearing on the application of the data protection legislation. Any organization collecting personal data of data principals will need to publish a privacy policy. An exception is provided to small entities where processing of personal data is not automated. (Smaller entities are yet to be classified by the Data Protection Authority)

   b) **the organization only collects email addresses to deliver newsletters?**

      Yes. An organisation that collects personal data requires a privacy policy.

   c) **the organization doesn't collect any personal data?**

      No, the organization doesn't need a privacy policy if there is absolutely NO personal data collection, including passive data collection.

   d) **the organization only has a contact form on the website?**

      Yes. Since the contact form will consist of personal communication details to get back to the individual, the organization will need a privacy policy.

   e) **the organization collects office email addresses of individuals?**

      It depends. If the office email address can identify the individual, a privacy policy is required since it is personal data. For example, the email address ravikumar@companyA.com may be categorised as personal data. If the email address refers to a specific position i.e. dpo@companyA.com , may not be categorized as personal data. Since most office email addresses are on the lines of the former example, it is advisable to publish a privacy policy.

Key considerations before drafting

1. **What personal data categories does the organization collect? Please consider all the services that are being offered to an individual.**

The PDP Bill categorises any data that directly or indirectly identifies an individual with regard to any specific characteristic, trait, attribute or any other feature or a combination of the same as personal data.

The data types under sensitive personal data of the SPDI rules have been modified to include official identifiers(any number or identifier attached to the data principal under a national or state law which can be used to verify the identity of the individual -like the Aadhaar number, PAN number), transgender status, intersex status, caste or tribe, religious or political belief or affiliation. Since official identifiers, transgender status, caste are some of the very

common data types collected, care has to be taken to ensure that they are explicitly mentioned in the sensitive personal data category in the privacy policy and are accorded the required protections.

The PDP Bill modifies the definition of personal and sensitive personal data to some extent. If an organization has been collecting personal and sensitive personal data, prior to the notification of the Bill, it will need to reassess the data that is being collected to verify if any of the data types fall into the newer definitions. If an organization is starting the processing operations post the notification of the Bill, the procedure to identify the personal data categories being collected remains the same.

Surnames as sensitive personal data: One question that is often asked in the Indian context is if surnames should be classified as sensitive personal data due to their ability to reveal the caste of the individual. Till additional guidance from the Data Protection Authority of India is obtained, it is advisable to categorise surnames as sensitive personal data in cases where the purpose of processing is based on the caste of the individual. In the absence of a direct relation between the surname and the purpose of processing, it may be prudent to either delete or if that is not possible then to correctly and properly anonymise the surnames[22] instead of just classifying them as personal data.

Video surveillance for security and access control: Regardless of recording capabilities, the collection of images/videos through live video surveillance has the potential to identify an individual. Hence, the recordings as well as mere live surveillance shall be considered as personal data for the purposes of the proposed bill. In some cases the facial images being captured can be categorised as sensitive personal data if such images are a result of technical processing operations that are carried out on the individual to confirm their identity.

Passive data collection: It is relatively easier for the individuals to gather the personal data being directly collected since active disclosure from their end is essential. However, an individual will not be able to gather the data that is being automatically collected through passive tracking methods such as the use of cookies, web beacons, browser fingerprinting and other types of identification mechanisms. Hence, it is essential that organizations understand the functionality of their websites (even in cases where third parties are employed to operate the website) to ensure that all such passive tracking methods are included in the personal data collection in the privacy policy.

Although not an explicit requirement under the Indian legislation, a cookie policy that will aid the individual in understanding the nature of cookies engaged on the platform and their purposes combined with the ability to disable cookies that are not categorised as strictly necessary should provide more control over disclosure of data.

2. **Where does the organization collect personal data from?**

Based on the different types of personal data being collected(step1), identify and log the points where the individual is expected to actively disclose personal data and the points where the data is being passively collected. Records of such collection points will confirm that all personal data categories that are being collected have been identified. The record is also essential to determine the placement of the privacy notice/policy in the next steps.

3. **Why does the organization collect personal data?**

[22] Luc Rocher, ,Julien M. Hendrickx and Yves-Alexandre de Montjoye, “Estimating the success of re-identifications in incomplete datasets using generative models”, available at https://doi.org/10.1038/s41467-019-10933-3

Personal data has to be processed for a clear, specific and lawful purpose. The specificity depends on the context in which data is being collected and the data types that are being collected.

For example A: If a research organisation is collecting the email addresses of individuals to send newsletters: the level of specificity in the purpose need not be extremely high since it is a very simple activity. Hence, the privacy policy can merely state that the "personal data provided shall be used for sharing newsletters periodically." However, if the organization is using the email addresses and additional details such as geographical address, name etc. to analyse and create the profiles of individuals that are subscribing to its mailing list or send out customised newsletters and or other publication materials on the basis of the profile of the individuals it will need to provide the specifics of the processing operation.

The level of specificity will be higher in case of processing of sensitive personal data since the level of significant harm to the individual in the event of misuse of such data is higher. *For example B,* if an educational institution is required to collect details regarding the caste of the individual for entry based on their reservation policies the privacy policy must mention the same in clear terms. This will ensure that the individual knows that this data type is being used by the educational institution for one specific purpose.

The level of specificity also differs based on the complexity and opaque nature of the processing operation. *For example C:* Organization A is an e-commerce website and collects personal data to enable delivery of services as well as customise the offerings based on past purchases or browsing history. The purpose of the processing section in their privacy policy states that "personal data collected will be used to improve their services." This statement does not indicate the exact nature of activity that will be performed in their effort to improve their services. It is not possible for an average consumer to be aware of the operations that would enable such "improvement in services". In case of complex operations, a vague purpose will not provide enough clarity regarding the purpose of processing to the individual.

Stating a vague purpose in the privacy policy can be appealing as the repeated consent or compliance with a fresh legal basis of processing can be avoided which will give the organization more leeway to use the data collected. However this is highly discouraged and can violate the provisions of the law.

Following is one format through which purpose can be stated in the privacy policy (for Example B):

(indicative list)

Purpose	**Personal Data Categories used**
Emergency contacts	Details of guardians/parents/emergency contacts
Determining scholarship amounts	Details of parents, IT returns of the household, name of student
Validity of admissions through reservation policy	Name of student, identification documents to prove caste

4. Based on the purposes identified, which lawful basis of processing can the organization rely on?

The PDP Bill identifies eight lawful bases of processing personal data.[23] These bases provide the legal legitimacy to the purpose of processing that has been identified. The guidance document expands on only two out of the eight, i.e. processing based on consent and existing legislation, as the rest need additional guidance from the data protection authority of India.

Can the organization rely on consent?

Processing personal data based on the lawful basis of consent is valid only if consent is free, informed, specific, clear and capable of being withdrawn. The privacy policy is examined to determine if the consent provided is *informed*. The specificity of the purposes identified is examined to determine if consent is *specific*. Consent based on a policy that omits crucial details mandated by the proposed bill will not be valid. The freedom to exercise choice based on the relationship between the individual and the entity seeking consent, potential vulnerabilities of the individual while providing consent, presence of misrepresentation and fraud is examined to determine if the consent is *free*. *For example D:* The power imbalance between employers and employees can make it difficult for the former to process the personal data of the employees solely based on consent.

An affirmative action has to be taken by the individual to provide their consent for it to be *clear*. This is usually done either through opt-in boxes or explicit affirmative statements. It is essential that consent for a particular purpose is not bundled with an incompatible purpose. *For example E:* An e-commerce website requires the customer to consent to the use of their email address to deliver shipping updates post sale. However, if delivering shipping updates has been tied to providing marketing updates to the customer and the latter is not incidental to the main purpose of processing, consent will be invalid.

Is there an existing law that requires the organization to process the personal data?

This legal basis can be relied on if there is an existing legislation that requires the organization to process the personal data of the individual. For example: Employers may need to collect the PAN card details of the employees to cut TDS for the Income Tax Act.

5. Who does the organization share data with?

This section intends to highlight the third parties employed by the organization that might have access to the personal data being provided by individuals. A list of third parties that are currently employed that either perform services on the organization's behalf or assist them in performing some of the services should be published in the privacy policy. This list should be regularly updated. Relying on language such as "data will be shared with affiliate companies" or providing illustrative lists is discouraged.

Following is one format through which the list of third parties along with purpose of processing can be provided:

(indicative list)

Name of the purpose	Third parties involved	Additional details

[23] S. 12

Delivering newsletters	e-champ	Details regarding their data retention, data security, personal data they have access to is available here (Link)
Website functionality	XYZ ltd	Details regarding their data retention, data security, personal data they have access to is available here (Link)

6. **How long does the organization intend to keep the personal data collected?**

Organizations are expected to delete the personal data collected after the purpose of processing is completed. However, in many cases the same details are stored for continued services. In such cases, if the legal basis for processing is consent, the personal data can be retained till consent has been withdrawn.

In some cases legal obligations can mandate the organization to store certain data types for a specific amount of time. Care has to be taken to ensure that only those data types are retained and the rest of the data is either anonymised or deleted. These considerations should be clearly mentioned in the privacy policy along with the names of the specific legislations that are required to retain data after purpose is fulfilled.

7. **Does the organization have a dedicated email address/process through which individuals can exercise their data principal rights?**

Communication details to be mentioned in the privacy policy. Currently, PDP 2019 doesn't state the time period within which the data fiduciary is expected to respond to the data principal. Post notification of the Regulations, it would be prudent to state the time period in the privacy policy.

8. **Does the organization have a dedicated grievance redressal mechanism for privacy complaints and queries regarding the data processing operations?**

The details of the position and contact details to be mentioned in the privacy policy.

9. **What are the existing security measures in place?**

Include the details in simple and not technical language. Include security measures of third parties (if any)

Key considerations during drafting

After gathering all the above mentioned details, following are some of the key considerations for the drafting stage:

Language

The purpose of a privacy policy is moot if it cannot be comprehended by individuals disclosing data. The importance of simple accessible language becomes more important in

cases where complicated operations are performed to offer services. Organizations are advised to:

- Refrain from using purely legal language
- Refrain from using words that paint an ambiguous picture regarding the data being processed such as “we may use your data for …”, “ we collect personal data including but not limited to”, “personal data such as name, PAN Card and other such data types”
- Customise the language of the policy for their audience

Multiple languages

The proposed Bill requires organizations to provide privacy policies in multiple languages, where necessary and practicable. Even though further guidance on the contours of the necessity and practical phrase can be expected from the Data Protection Authority of India, international best practice can be referred to for the time being. It is suggested that organizations should resort to translating privacy policies in multiple languages wherever the organization targets individuals speaking those languages[24]. It is acknowledged that such a practice can be impractical in a diverse country like India. However, an attempt should be made to at least translate the policy into some of the major speaking languages in the country based on services provided.

The primary characteristics of a valid privacy policy i.e. “clear, concise and easily comprehensible” apply to the translated privacy policy as well. It is vital that the translation is done by professionals and not just an online tool to ensure that it remains accurate.

Structure

Following are some of the methods based on which the policy can be structured:

- *Layered approach*

As the name suggests, the policy can have multiple layers wherein the first layer provides the individuals with the highlights of the processing operations and the subsequent layers provide more specific details based on the individual’s preference[25]. This however is not an excuse to bury important details under the subsequent layers. Any information that could have an effect on the practices of the individual should be provided in the first layer.

- *Just in time notices*

These notices appear at the data collections points and are customised to the personal data type that is being collected. For example: A pop up box next to the text field where the individual provides an address can be displayed with a sentence or two on how that address will be used. A link to the full privacy policy can be provided in the pop up box.

- *Consideration for policies displayed on mobile phones*

The limitations of the diverse range of mobile phones should be considered while drafting the policies. The text of the policy should be large enough to read clearly. Additional audio and video functionalities of mobile phones can also be used to communicate the policy. However, care should be taken to adapt it to the average attention span of the individual.

[24] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/how-should-we-draft-our-privacy-information/

[25] This privacy policy can be referred to understand the practice of layered policy.

- *Design concerns*

The readability of the policies can be enhanced by the presence of section separators to differentiate between the types of content. Visual summaries of the policies are encouraged for better reach with the individuals[26]. The policy should be comprehensible via screen readers.

- *External review*

Prior to finalising and publishing the policy, it is advisable to select a sample of members from a typical audience of the service/platform and proceed to test the effect of the policy. The sample should be asked to access and read the policy without any assistance to receive feedback. Necessary changes based on the feedback can be made.

Key considerations after drafting

The privacy policy has to be treated like a live document.

- Periodic checks of compliance with internal processes need to be conducted. In the event of any meaningful change in either the purpose of processing or any of the details mentioned in the privacy policy(such as employing a data processor), the document will need to be updated. The organization will also have to version control the document.

- An update notification will have to be sent to the data principal. The notification should contain the effective date of the updated privacy policy, brief details about the substantial changes in the processing operations and options to register grievances or withdraw consent if the individual doesn't want to accept the changes.

- In case of any substantial change in the data processing operation, the personal data should be processed in the new way only after the data principal has been given a reasonable opportunity to withdraw consent.

[26] https://cis-india.org/internet-governance/blog/design-concerns-in-creating-privacy-notices