PACTA

SOCIAL | IMPACT | LEGAL

Digital Personal Data Protection Act 2023

A Primer for NGOs

Section 1 - Introduction

Pacta had written about the Digital Personal Data Protection Bill 2022[1] (DPDP Bill 2022) and its implications for the social sector in India. On August 11, 2023,[2] the modified version of the Digital Personal Data Protection Act 2023 (the Act/ the DPDP Act) was notified in the official gazette after being passed by the Parliament and receiving Presidential Assent. However, for the Act to be implemented in spirit, the allied rules would need to be notified.

We have observed a surge in interest from the social sector to understand the Act, its implications on NGOs and how NGOs can navigate the compliances under the new digital data privacy law. Pacta has created this Primer as a guide for nonprofit organizations in understanding the application and effects of India's Digital Personal Data Protection Act, 2023.

The Union Government has notified the Act in the Official Gazette, but the date on which it will come into force has not yet been announced. Until then Section 43 A of the Information Technology Act 2000, read with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, will govern questions of data privacy.[3]

[1] https://www.pacta.in/blog/Digital-Personal-Data-Protection-Bill--Implications-for-Civil-Society-Organisations.htm
[2] https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
[3] https://www.pacta.in/blog/Data-Protection-for-Civil-Society-Organisations.htm

Section 2 - Application of the Digital Data Protection Act to NGOs

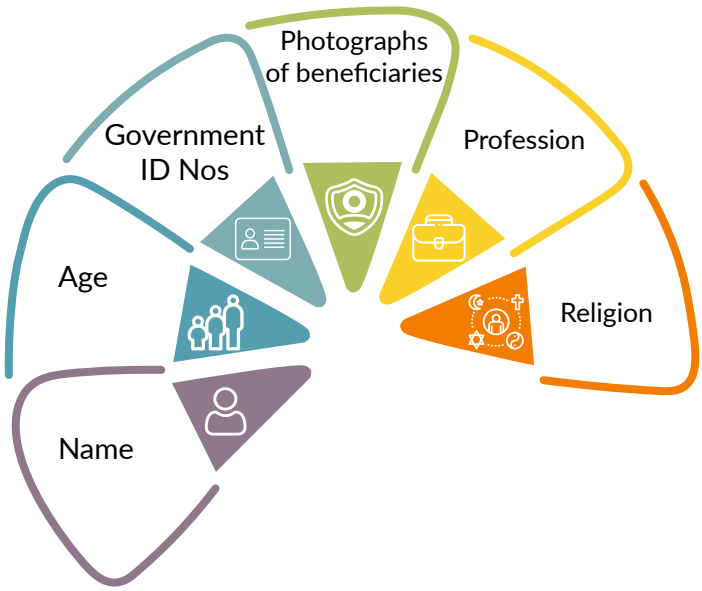
The Act will apply to the processing of Personal Data collected in India in two situations:

i. when Personal Data is collected online from Data Principals, and

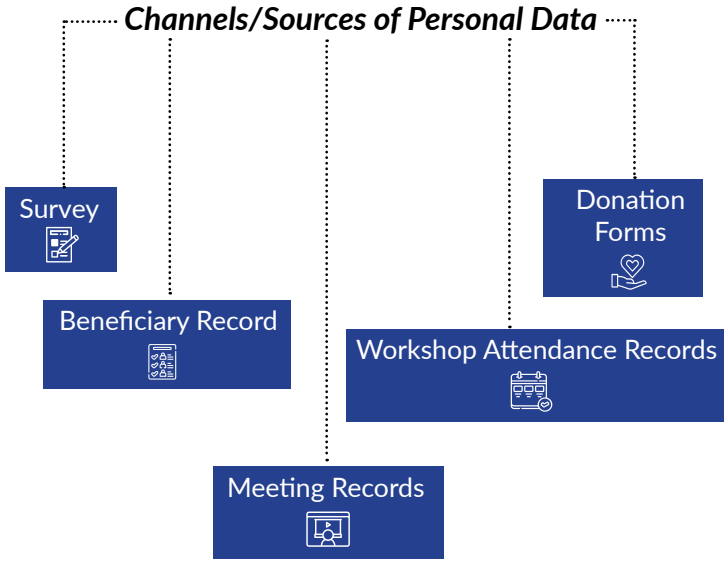
ii. when Personal Data is collected offline and then transferred to a digital format.

The Act will also cover processing personal data outside of India if that processing is related to profiling people in India or offering goods and services to data principals in India.

Examples of data collected by NGOs



Channels/Sources of Personal Data



NGOs indulge in the above activities of collecting and processing of Personal Data. **Thus the Act will** apply to all nonprofits and charitable organizations that collect personal information from their stake-holders online or offline and then digitize it.

There are exceptions:

The provisions of the Act does not cover:

i. Personal data managed by individuals for their own purposes,

ii. Personal Data that is intentionally made publicly available by the individual it pertains to or by someone who's legally obligated to share such data.

Illustration:1

Y, an individual, has voluntarily shared personal details on a public forum while participating in an online discussion. In this scenario, the regulations outlined in this Act would not be applicable.

Section 3 - Data Privacy Jargon Debunked

A. Data Principal: The individual to whom the personal data belongs, which includes the child's parents or legal guardians if the person is a child (less than 18years of age) or person with disability.

B. Data Fiduciary: Any person who, alone or in collaboration with others, determines the purpose and means of processing Personal data are referred to as a Data Fiduciary. ***Therefore, non-profit organizations or charities would assume the role of data fiduciaries.***

C. Data Processor: Any person who processes personal data on behalf of a Data fiduciary (this includes research agencies or data scientists engaged by NGOs).

D. Digital Office: Refers to an office that utilizes an online system for carrying out activities, starting from receiving notifications, complaints, references, directions, or appeals, and continuing until the resolution of these matters, all of which occur through online or digital means.

E. Digital Personal Data: Refers to Personal Data in a digital format.

F. Personal Data: Any information about a person who can be identified by or in connection with that information. (Eg. name, age, address, email address, Aadhar number)

G. Significant Data Fiduciary: Pertains to a Data Fiduciary or a group of Data Fiduciaries that the Central Government designates. This designation is determined by considering factors such as the quantity and sensitivity of processed Personal data, the potential risks to the rights of Data Principals, the possible impact on India's sovereignty and integrity, risks to electoral democracy, state security, and maintenance of public order.

Section 4 - How Did Data Privacy Become a Mainstream Conversation in India

In India, the right to privacy is said to be enshrined under the fundamental right to life. In a landmark judgement delivered by the Supreme Court in K.S. Puttuswamy v. Union of India it was held that right to privacy includes informational and technological privacy. In particular, the right to identification, the right to control the broadcast of personal information, the right to be forgotten, and the privacy of children are all included in the right to privacy.

There are data privacy laws in place in over 130 countries around the world. Some of the most notable data privacy laws include- General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) in the United States applicable to businesses, Personal Data Protection Act (PDPA) in Singapore, etc.

Anu Bradford, a law professor at Columbia University, coined the term ***"Brussels Effect"*** to describe the phenomenon of European rules becoming global standards. She argues that this is because it is easier for companies to apply European rules across their entire organization, rather than having to comply with different rules in different countries. The Brussels Effect is often seen as a form of soft power. Therefore, India's Data Protection Act 2023, has similar concepts which are found in GDPR.

Section 5 - Data Privacy Laws - Two Key Ingredients

Two concepts intrinsic to data privacy are - **Consent and Notice**

1. Consent: Consent is the primary basis for the processing of Personal Data. For Personal Data to have lawfully collected from a person, consent must be:

i) freely given,

ii) taken for a specific purpose,

iii) taken with full information as to why it is collected, how it will be used, who will have access,

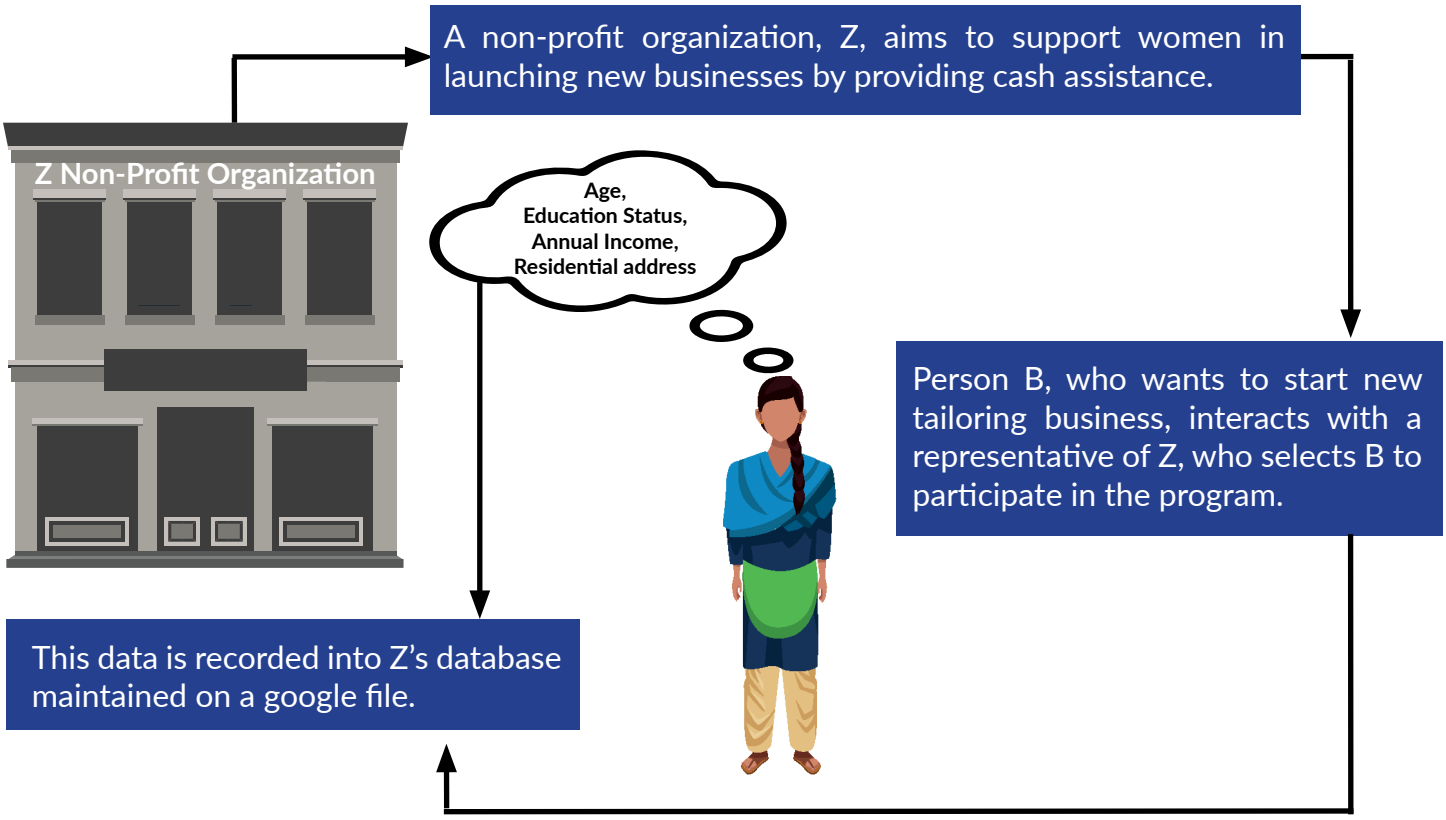
iv) taken unconditionally (not involve a threat)

2. Notice: Each request for consent must be accompanied by a notice from a Data Fiduciary. This notice should provide information about the process of withdrawing consent, the procedure for addressing grievances, and how to file a complaint with the Data Protection Board (Board). The format and additional details for this notice will be determined by the Central Government, introducing a novel aspect in the DPDP Act 2023.

Note:

NGOs may have an on-going data-collection exercise, where an NGO did not originally give notice or take consent at the time of establishing the data-collection pipeline. To address this, the Act provides for a comparable notice, to be provided as soon as it's ***"reasonably practicable,"*** after the DPDP Act 2023 comes into effect. The law doesn't define a specific timeframe for such retrospective notice and consent, and leaves it as subjectively ***"reasonable".***

Illustration:2



Implication:

Prior to collecting the information, Z must ensure that a notice is given to B. This notice should outline what data is collected, why it collected. What it will be used for, who will have access to it etc, and shall take the explicit consent of Person B in wishing to disclose the information. If B has concerns on sharing specific information, Z's representative must understand the same and take steps towards addressing these concerns.

Actionable:

The notice given by NGO Z must also contain:

i) disclaimer on data protection,

ii) withdrawal of consent,

iii) grievance redressal mechanisms, and

iv) process of filing a complaint before the Data Protection Board.

Z should also ensure that employees accessing the data use the data only for the purposes it have been collected, and that unrelated persons even within NGO Z do not have access to personal information from the database.

Exception to take Informed Consent - Legitimate Use:

According to the Act, a data fiduciary is allowed to process Personal Data of a Data Principal without their explicit consent for certain ***'legitimate uses.'*** These encompass:

- Instances where a Data Principal willingly provides their Personal Data to a Data Fiduciary and has not conveyed their non-consent for the Personal Data's utilization.

Illustration:3

An NGO, X, collects Personal Data from an individual, Y, who donates.

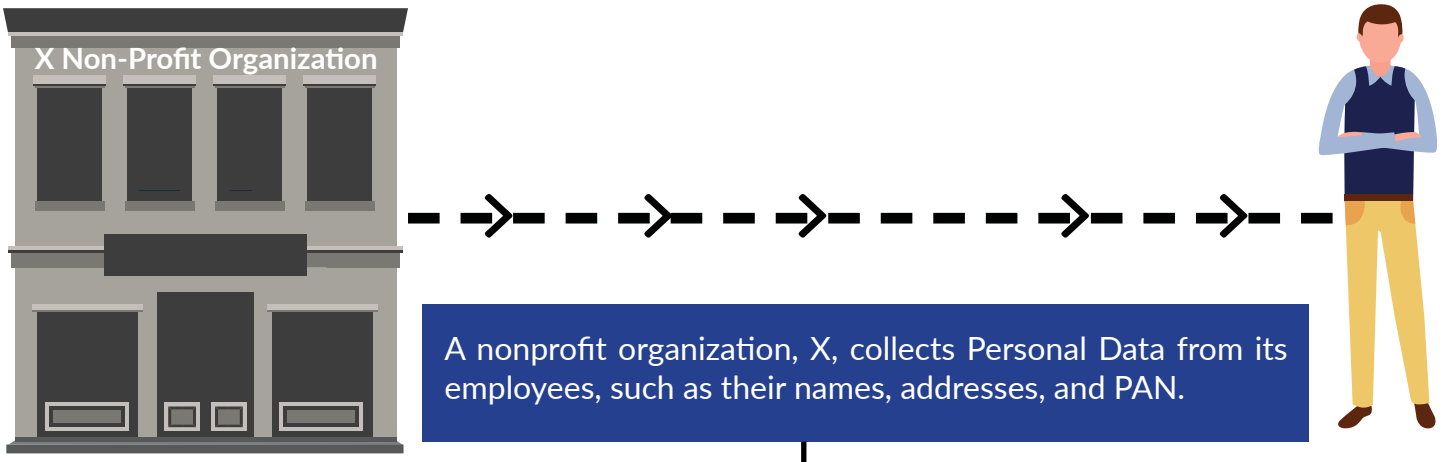
Y voluntarily provides their personal data and requests X to acknowledge receipt of the donation by sending a message to their mobile phone.

Implications:

NGO X is permitted to use Y's phone number for the purpose of sending a receipt, without an explicit consent therefor.

- Situations related to employment or aimed at safeguarding an employer against potential loss or legal responsibility. The terminology ***"safeguarding an employer from loss or liability"*** is a new addition in the DPDP Act 2023, focusing on aspects like corporate espionage and the protection of proprietary rights.

Illustration:4



A nonprofit organization, X, collects Personal Data from its employees, such as their names, addresses, and PAN.

Implications:

This data is used to process payroll, benefits, and other HR-related tasks etc and does not need explicit consent.

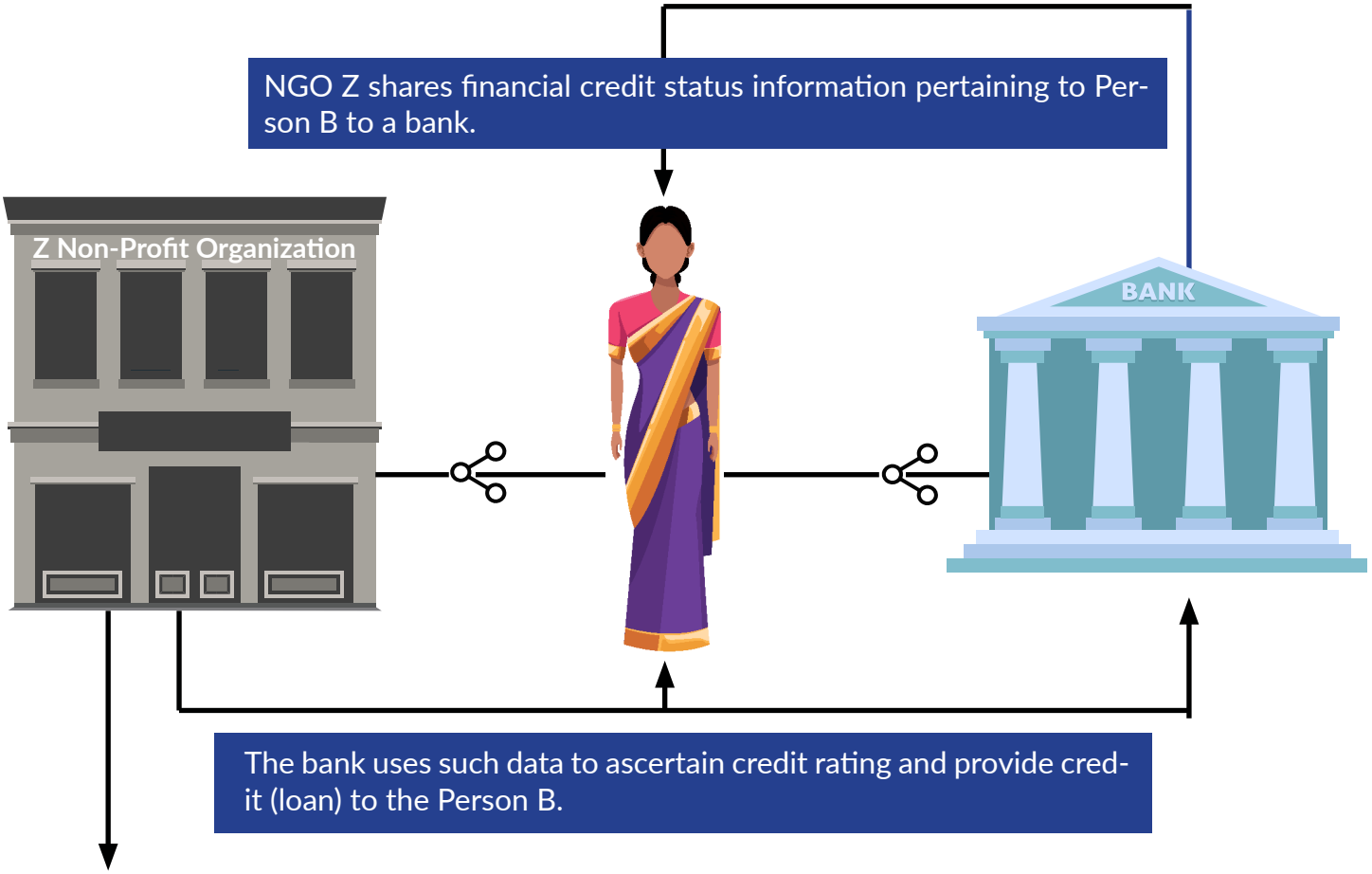
Section 6 - Data Fiduciary's Obligations under the Act

According to the Act 2023, Data Fiduciaries bear the primary responsibility for ensuring legal adherence in their processing activities (including those carried out by their data processors). Compliances are detailed below:

i. Accurate Information:

If the Personal Data is likely to be used by the Data Fiduciary to make a decision that ***"affects"*** the Data Principal or if the personal information is likely to be shared with another Data Fiduciary, the Data Fiduciary must exercise reasonable efforts to make sure that the personal information processed by or on behalf of the Data Fiduciary is accurate and complete.

Illustration:5



Implications:

NGO Z has a duty to ensure that data pertaining to Person B is accurate and complete.

ii. Security Measures:

The Data Fiduciary must take reasonable security precautions to prevent a breach of the Personal Data it has in its possession or under its control.

How to operationalise this: *NGOs can implement the following measures to ensure the security of Personal Data:*

1) *Provide access on a need to know basis*

2) *Store Data in password protected, preferably 2 factor authentication systems*

3) *Conduct a cyber audit to ensure that the network is secure and cannot be breached*

iii. Notify Data Breaches:

In the event of a Personal Data breach, Data Fiduciaries must promptly notify the Data Protection Board ("Board" hereinafter, which shall be constituted by the government) and each affected Data Principal. Failure to take reasonable security safeguards to prevent Personal Data breaches is punishable by a penalty of up to Rs. 250 crores and the failure to notify the Board in case of a data breach is punishable by a penalty of up to Rs. 200 crores.

As of now, there is no carve out exemption (with regard to applicability of the Act) for NGOs and so, the risk of a data breach can be too high and too steep for an NGO.

iv. Delete Data When No Longer Necessary:

The Act introduces specific guidelines for Data Fiduciaries to delete Personal Data, outlining instances where deletion is necessary – particularly when it's reasonable to assume that a designated purpose is no longer valid. Notably, the Act empowers the Central Government to establish timeframes for different classes of Data Fiduciaries, determining when a purpose can be considered as no longer valid – a novel aspect of the DPDP Act 2023.

v. Appointment of Data Protection Officer:

Data Fiduciaries must appoint a Data Protect Officer who would be responsible for addressing any queries from the Data Principals regarding their Personal Data. This Data Protection Officer is to be based out of India only if the Data Fiduciary falls within the definition of a Significant Data Fiduciary

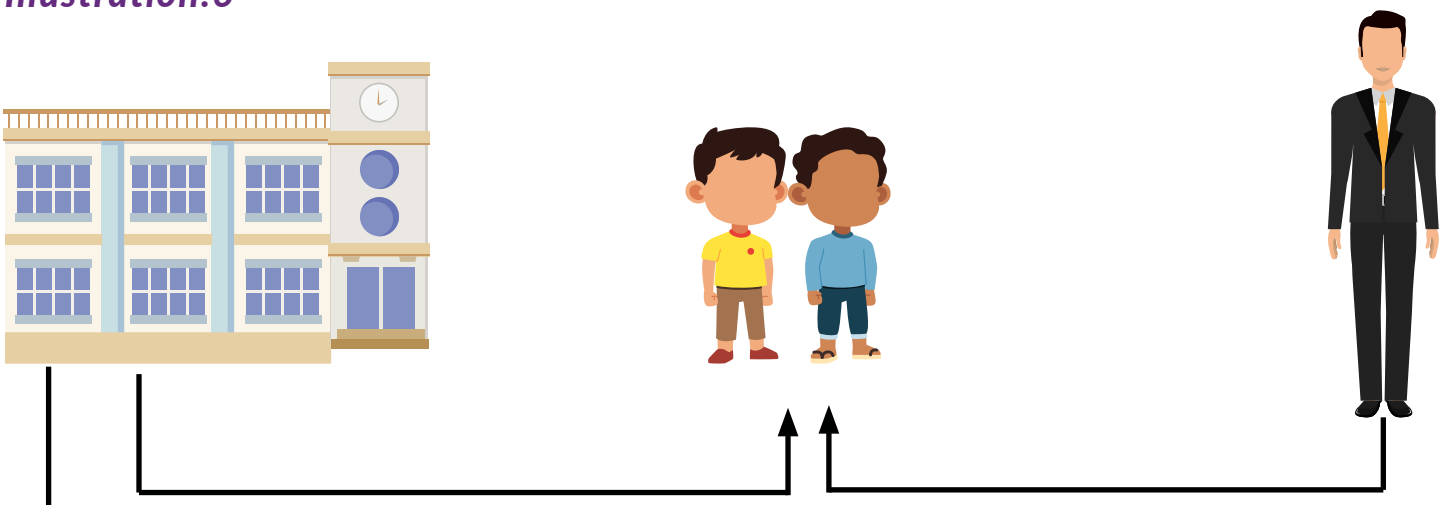
vi. Grievance Redressal Mechanism:

The Data Fiduciary shall establish an effective mechanism to redress the grievances of Data Principals. The Act does not prescribe any specific process or timelines for grievance redressal, and this might be notified by the Rules later.

vii. Cross-Border Transfer:

Under normal circumstances, Data Fiduciaries can transfer Personal data to any country except those regions that might be officially notified as restricted destinations by the government in the future.

Illustration:6



A nonprofit that provides educational services to children in India is conducting a research on a new program that has been piloted.

The Researchers collect personal data from its students, such as their name, contact information, and academic records. One Researcher based in the United States who has the skills for quantitative analysis, wants the database emailed to them so that they can conduct the analysis

Implications:

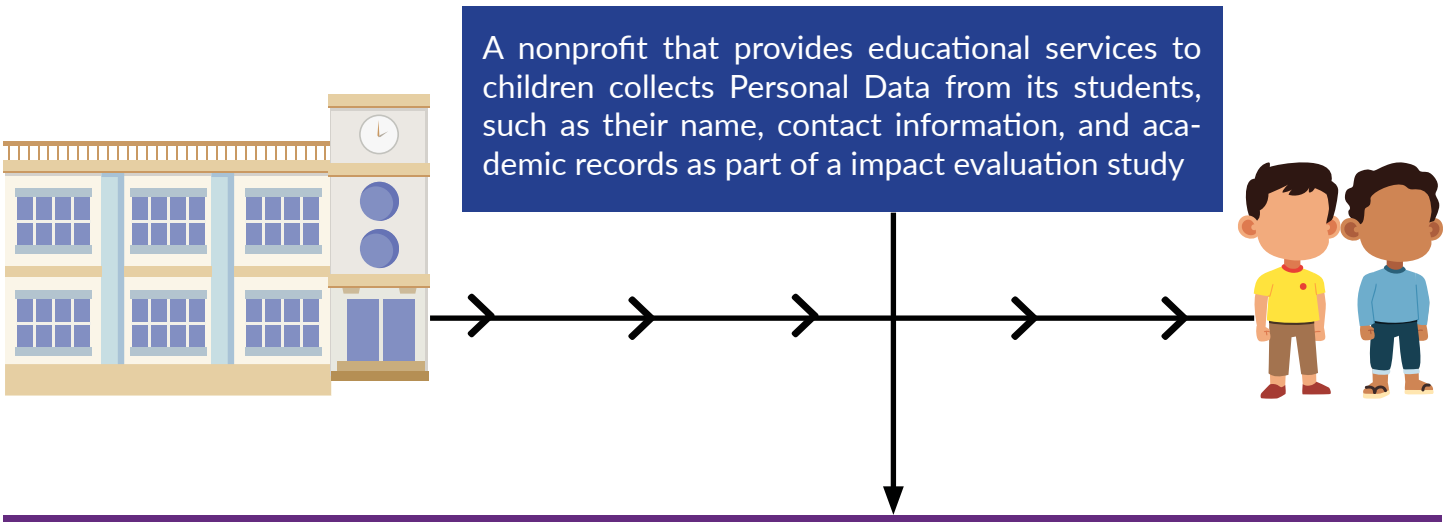
To comply with the Act, the nonprofit must first check if the United States is a country or territory that the Central Government has notified as being not a safe destination for the transfer of personal data. If it is not notified, then the nonprofit can transfer the Personal Data. This list of countries will be notified shortly.

viii. Children's Data/ Data of Person with Disability:

Data fiduciaries have the additional obligation to obtain verifiable parental consent or consent of the lawful guardian while processing the personal data of a child or data of a Person with Disability. Data Fiduciaries must refrain from data processing that would cause any detrimental effect on the well-being of a child and also refrain from tracking, monitoring, and targeted advertising aimed at children. Failure to adhere to this attracts a penalty of up to INR. 200 crores.

As per the 2023 Act, the Central Government is also empowered to notify the age above which certain Data Fiduciaries will be exempt from these obligations, if it is satisfied that the processing of children's Personal Data is carried out by a Data Fiduciary in a ***'verifiably safe'*** manner. ***Thus NGOs working with children and people with disability have the additional responsibility to comply with this provision.***

Illustration:7



Implications:

To comply with the DPDP Act 2023, the nonprofit must obtain verifiable parental consent before processing the personal data of its students.This can be done by sharing a consent form with the parents, or recording the explicit parental consent in the survey form.

The nonprofit is not permitted to use/ sell the data to target its students with advertising. The nonprofit should also ensure that the processing of its students' Personal Data does not cause any detrimental effect on their well-being. This would mean broad and sweeping obligations for NGOs to protect data pertaining to children and people with disabilities.

Section 6 - Right of the Data Principal

The Act grants the data principal the right to:

i) access information from their Data Fiduciary about their Personal Data processed by the data fiduciary to whom the consent has been given or where the consent has been assumed.

ii) ask for correction, completion, updating, or erasure of their Personal Data from the Data Fiduciary, unless the retention is necessary for the specified purpose.

iii) seek readily available means of grievance redressal provided by a Data Fiduciary or Consent Manager only after exhausting all these remedies the Data Principal shall approach the Data Protection Board, and,

iv) Nominate any individual to exercise his rights upon his death or incapacity.

It is important to note that these rights might be subject to limitations in cases where processing is carried out based on 'legitimate use' grounds.

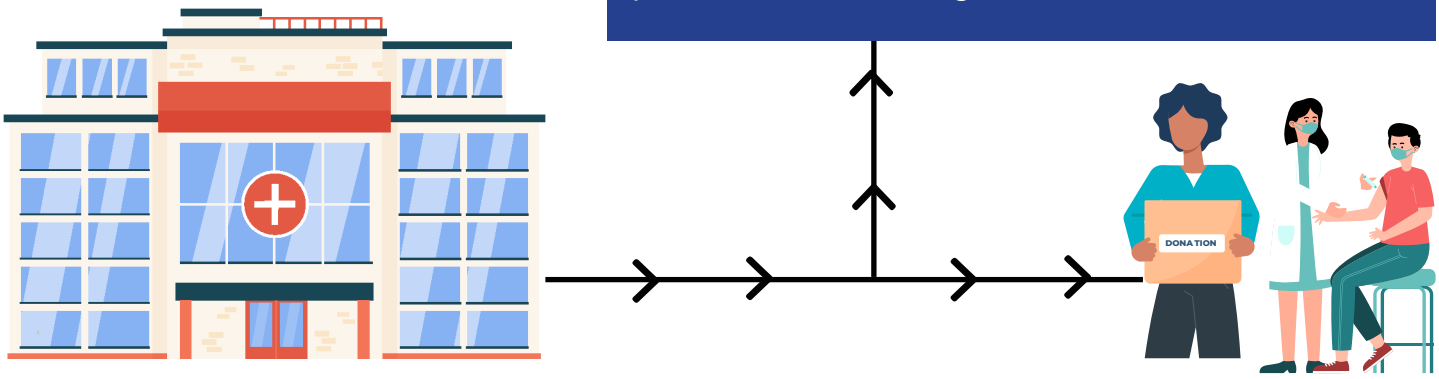
Note:

Depending on the volume and nature of data processed, the Central Government has been vested with the power to exempt certain fiduciaries from issuing notice before consent, ceasing to retain data after the purpose has been served, accuracy, the provision related to children, and the Data Principal's right to information about his Personal Data. However, the Act does not indicate what kind of fiduciaries will be granted the benefit of the exemption. One might hope that NGO's are exempted from some or all obligations under this new law.

Illustration:8

healthcare organization

An NGO working as a healthcare organization that provides medical services and support to individuals in need. This organization collects Personal Data from patients, donors, and volunteers for various purposes, including patient care, fundraising, and volunteer coordination



Implications:

a. Access to Information: A patient has the right to access their medical records and other relevant information that the nonprofit has gathered during their treatment. They can inquire about their diagnosis, treatment history, and prescriptions.

b. Correction and Erasure: A patient (say a TB survivor) might notice that their data (say TB positive status) information in the nonprofit's donor database is incorrect. They can request the correction of this information. A former volunteer may decide that they no longer want their volunteer history to be retained by the organization and can request erasure.

c. Grievance Redressal: Suppose a patient is dissatisfied with the way their medical data was handled during their treatment. They can use the nonprofit's provided grievance redressal mechanism to express their concerns. The nonprofit is obligated to respond promptly and address the patient's issues.

d. Nomination of Representative: An elderly patient might appoint a family member as their representative to exercise their data rights if they are unable to do so due to health reasons. This ensures that someone they trust can manage their data-related matters.

Section 7 - Some More Jargon To Catch Up With

1. Significant Data Fiduciary

The law maintains its recognition of a distinct category known as Significant Data Fiduciaries or 'SDF, designated by the Central Government based on specific criteria. SDFs carry additional responsibilities, including:

i) Conducting periodic audits.

ii) Undertaking assessments of data protection impact.

iii) Appointing an independent data auditor and a data protection officer.

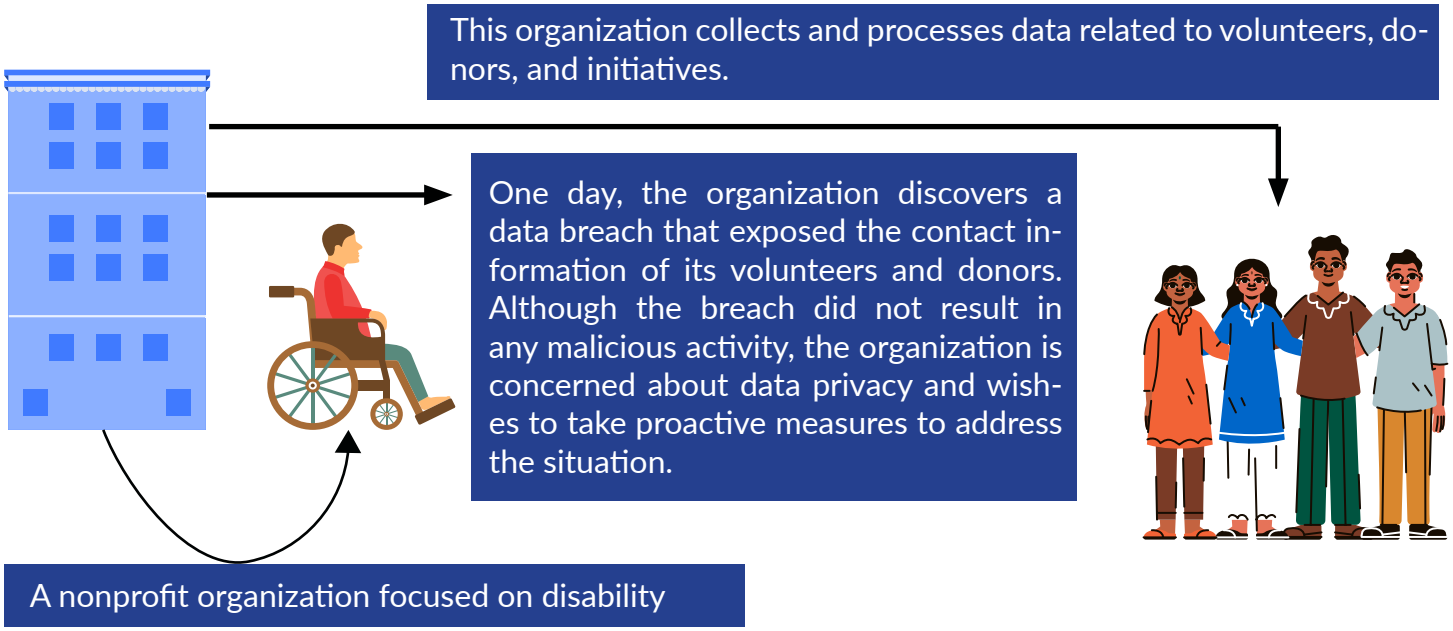
Implications:

In this context, if an NGO falls under the category of a SDF, the NGO would have to appoint a 'Data Protection Officer' who is an individual situated in India and answerable to the Board of Directors or the relevant governing body of the SDF. The Data Protection Officer also functions as the main point of contact for the grievance redressal mechanism established by the SDF.

2. Voluntary Undertaking

At any time (especially if an NGO realises there has been a breach of its obligations under the data privacy law) , anyone can give the Board a voluntary undertaking that they would follow any part of the Act. The Board has the discretion on whether to consider the undertaking or not. Such a voluntary undertaking may be publicized. The explanatory note published along with the Act considers this provision as a measure to encourage timely admission and rectification of lapses. The focus of the Act is on enabling and facilitating compliance rather than penalizing non-compliance. So, it is a way for the Data Fiduciary to fix a breach at any time after it has happened and keep the Board from taking action against them.

Illustration:9



Implications:

In line with the provisions of the Act, the nonprofit organization should give a voluntary undertaking to the Data Protection Board. In the undertaking, the NGO must outline the steps they will take to address the breach, ensure data security, and prevent future incidents.