PACTA
SOCIAL | IMPACT | LEGAL

Chitta
Initiative for Research by Pacta

Understanding the DPDP Act, 2023 and Rules, 2025:

A Primer for Non-profits

Why a Primer on the Digital Personal Data Protection Act for Non-profits?

Non-profit organisations routinely collect, store, and process personal data in the course of delivering programmes, conducting research, engaging with beneficiaries, managing donors, and coordinating with partners. This data often includes sensitive personal information, and its responsible handling is critical not only for legal compliance but also for maintaining the trust and dignity of the communities they serve.

India's Digital Personal Data Protection Act, 2023 (DPDP Act) introduces a comprehensive legal framework governing the processing of digital personal data. The law establishes specific obligations for entities handling personal data, including requirements relating to lawful consent, purpose limitation, data security safeguards, grievance redressal, and accountability. While the Act applies across sectors, its implications for non-profit organisations are distinct. Many organisations in the social sector operate with limited legal, financial, and technical capacity, yet handle significant volumes of personal data as part of programme delivery, research, advocacy, and service provision. The introduction of new compliance obligations therefore necessitates accessible, sector-specific guidance to help non-profits understand and implement the law effectively.

The DPDP Act was notified on August 11, 2023 and while it established the overall legal framework and defined the roles and responsibilities of Data Principals, Data Fiduciaries, and Data Processors, its operationalisation depended on the notification of detailed Rules. The Ministry of Electronics and Information Technology released the draft Digital Personal Data Protection Rules, 2025 on January 3, 2025, for public consultation, inviting feedback from stakeholders across sectors. Following an extended consultation process, the final Rules were notified on November 13, 2025, paving the way for the phased implementation of India's data protection regime (See Box 1).

Pacta has closely tracked the development of India's data protection framework and its implications for the social sector. Following the release of the Digital Personal Data Protection Bill, 2022, Pacta published an initial primer analysing the Bill[1] and outlining its anticipated impact on non-profit organisations. After the enactment of the Digital Personal Data Protection Act, 2023,[2] Pacta continued its engagement by developing explanatory resources to help organisations understand the structure of the law and prepare for compliance. As part of the public consultation process on the draft Rules in 2025, Pacta also submitted detailed comments,[3] focusing on the operational realities and constraints faced by social sector organisations, as well as considerations relating to the rights of persons with disabilities.

---

[1] https://www.pacta.in/post/digital-personal-data-protection-bill-implications-for-civil-society-organisations
[2] https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
[3] https://e6a1ddce-638a-4c2a-a468-3bb06cb66ec2.usrfiles.com/ugd/0e1e8f_dac3c556ab8d4ecba1026b43d60e2bbc.pdf

Following the notification of the final Rules, which clarified the operational requirements and implementation timelines under the law, Pacta developed this Primer. This Primer is specifically intended to support non-profit organisations in understanding the application and effects of the Digital Personal Data Protection Act, 2023, and to enable them to navigate the emerging compliance landscape with clarity, confidence, and contextual relevance to the social sector.

Box. 1: Timeline for Implementation of the Digital Personal Data Protection Act

The Rules provides a staggered timeline for the implementation of various provisions:

- Clauses relating to the Data Protection Board and Definition clauses come into effect immediately. (November 13, 2025)
- Rule 4, relating to the registration and obligation of consent managers, come into effect one year from publication of the Rules. (November 13. 2026)
- All other Rules, including the obligations for all other organisations, come into effect eighteen (18) months from publication of the Rules. (May 13, 2027)

Disclaimer: This primer aims to provide general guidance to NGOs navigating compliances under the DPDPA. For detailed advice, non-profits are encouraged to refer to the full text of the Act and its amendments and consult legal experts as needed. The authors are not liable for any errors or omissions.

Suggested Citation: Pacta. (2026). Understanding DPDP Act, 2023 and Rules, 2025: A Primer for Non-profits

Table of Contents

Section 1 - Introduction

In an increasingly digital world, Personal Data has become both a powerful resource and a profound responsibility. In India, the enactment of the Digital Personal Data Protection Act, 2023 (DPDPA) marks a historic shift in how Personal Data is governed, processed, and protected. For the first time, we have a comprehensive, cross-sectoral data protection law that establishes clear rights for individuals and clear obligations for organisations that handle their data. For social sector organisations, this law is especially significant, as they often work with some of the most vulnerable populations and routinely collect and process sensitive personal information, including health information, financial details, identity documents, photographs, and impact data. The DPDPA brings such processing within a structured legal framework, requiring transparency, purpose limitation, data minimisation, security safeguards, and respect for individual rights.

This Primer is designed to help social sector organisations understand the DPDPA in practical, operational terms. It aims to provide actionable guidance to help organisations create mission-aligned data protection practices. By embedding responsible data governance practices into everyday operations, social sector organisations can enhance beneficiary trust while demonstrating accountability to donors and regulators. In complying with the DPDPA, organisations can reaffirm their core values: respect for the dignity and rights of every individual whose life and data you touch.

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

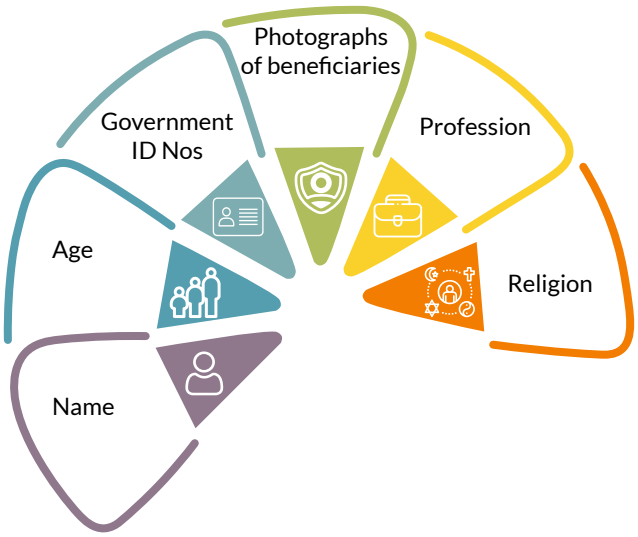
The Act will apply to the processing of Personal Data in India:

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

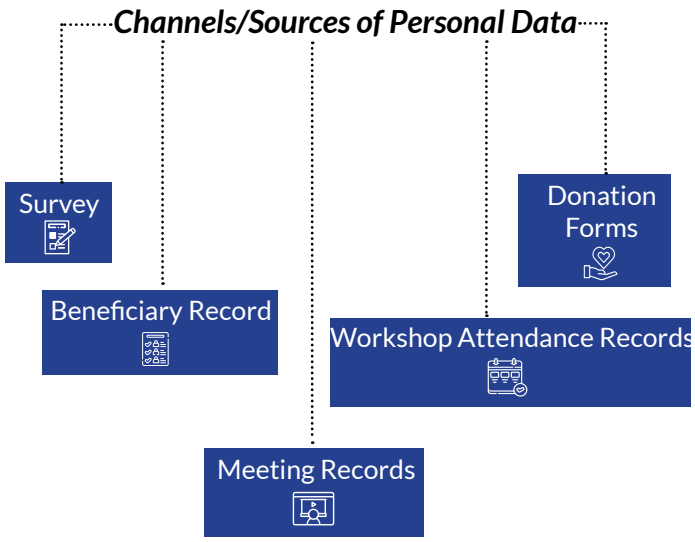
ii. when Personal Data is collected offline and then transferred to a digital format.

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 often engage in the above activities of collecting and processing of personal data. Thus, the Act will apply to all non-profits and charitable organisations that process personal data, either directly through digital means or if they collect the data through physical means and subsequently digitize it.

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 organisations or charities are likely to 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 utilises 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 is referred to as Digital Personal

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, Aadhaar number)

G. Significant Data Fiduciary: 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.

H. Consent Manager: A person registered with the Data Protection Board of India that serves as a neutral, single point of contact to facilitate the Data Principal in giving, managing, reviewing, and withdrawing consent. This is done through a platform that is accessible, transparent, secure, and interoperable across Data Fiduciaries, thereby ensuring ease of consent management in accordance with the principles of informed and meaningful consent.

I. Data Protection Officer (DPO): An employee of an organisation that ensures internal compliance with the Act and serves as the designated point of contact for Data Principals and the Data Protection Board. Significant Data Fiduciaries must mandatorily appoint a DPO.

J. Data Breach: Any unauthorised or accidental access, disclosure, alteration, loss, or destruction of personal Data that compromises the confidentiality, integrity, or availability of that data.

K. Data Protection Board of India: A statutory body to be established under the Act to enforce compliance, adjudicate violations, and impose penalties. The Board will operate digitally, and shall have the power to conduct inquiries, issue directions, and ensure that rights of Data Principals are upheld.

L. CERT-in: The Indian Computer Emergency Response Team as set up under the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013. CERT-In functions under the Ministry of Electronics and Information Technology and is the nodal agency for responding to computer security incidents as and when they occur. Any individual or entity affected by a Cyber Security Incident may report the same to CERT-In, and certain Cyber Security Incidents must mandatorily be reported. CERT-In then addresses these incidents and provides support depending on the type and severity of incident, affected entity, available resources, etc.

M. Cyber Security Incident: Any real or suspected adverse event related to cyber security that results in unauthorised access to the Data Fiduciary's systems or resources, disruption of operations, misuse of computer resources leading to data leaks or unauthorised data access in violation of confidentiality norms, or unauthorised alteration of data or information.

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

The Supreme Court of India, in its landmark 2017 judgement in the *K. S. Puttuswamy v, Union of India*[4], recognised that the right to privacy is a fundamental right under the Indian Constitution, intrinsically linked to the fundamental right to life. The Court further held that the 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 has been increasing recognition of the importance of citizens' right to privacy across the globe, with legislations on this subject being put into place in over 130 countries. 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 and Personal Data Protection Act (PDPA) in Singapore.

The prevalence of such legislation has also led to multinational internet companies facing the prospect of having differing compliance requirements across the various jurisdictions that they operate in. 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 organisation, rather than having to comply with different rules in different countries. The Brussels Effect is often seen as a form of soft power, and, in the case of digital privacy legislation, has led to many countries basing their own domestic legislations on the GDPR. India's DPDPA is no exception, and uses, many concepts which are found in GDPR.

[4] 2019 (1) SCC 1

Section 5 - Data Privacy Laws - Two Key Ingredients

Two concepts intrinsic to data privacy are - Consent and Notice

1. Consent: Consent is often 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 after providing full information as to why it is collected, how it will be used, who will have access; and,

iv) taken unconditionally (not involve a threat)

2. Notice: Each request for consent must be accompanied by a notice from the Data Fiduciary. This notice should provide all necessary information about the data collection, including types of data being collected, the process of withdrawing consent, the procedure for addressing grievances, and how to file a complaint with the Data Protection Board (Board).

Obligation of Data Fiduciary to Provide Clear and Informed Notice to Data Principals

Before collecting or processing personal data, a Data Fiduciary is required to give a notice to the Data Principal (i.e., the individual to whom the data belongs). This notice must comply with the following standards:

i) Clarity and Independence: The notice must be accessible and understandable on its own, without requiring the Data Principal to refer to any other documents or communications. It must be presented in clear and plain language that any individual, regardless of legal background, can comprehend.

ii) Content of the Notice: The notice must include all necessary details to help the Data Principal make an informed and specific decision about giving consent.

At a minimum, this notice for consent should includes:

i) List of the categories of personal data being collected.

ii) The specific purpose for which the data will be processed.

iii) A detailed explanation of the goods or services to be provided or the uses enabled by processing the data.

iv) A direct communication link to the Data Fiduciary's website or app.

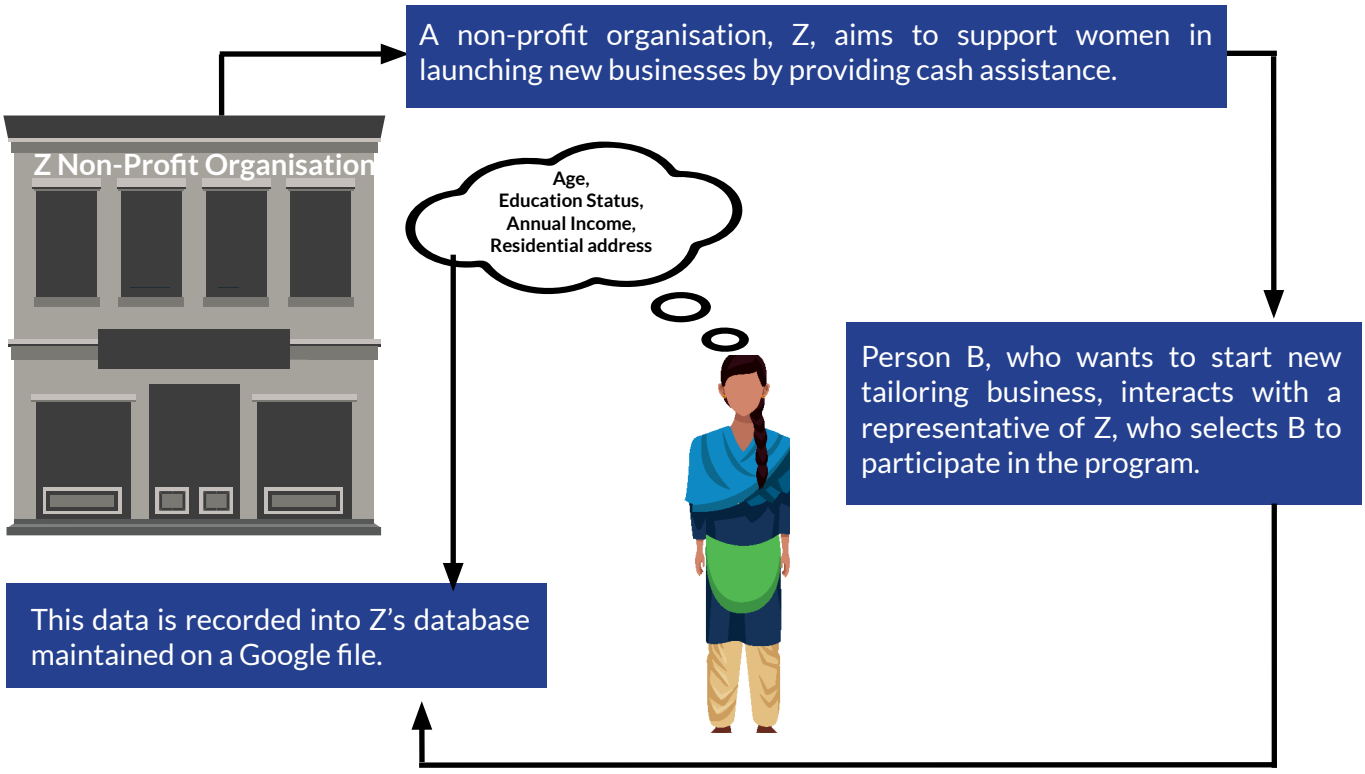
v) It should also describe any other available means through which the Data Principal can:

a) Withdraw consent—and this process must be as easy and accessible as giving consent.

b) Exercise rights under the Act (e.g., access, correction, erasure, or grievance redressal).

Illustration:1

Steps for Collecting and Using Personal Data : Consent and Notice



Implication:

Prior to collecting any personal information, NGO Z must issue a clear notice to Person B. This notice must be in plain language and provide a fair account of the following:

i) Itemised description of the personal data to be collected (e.g., age, education status, annual income, residential address);

ii) Specified purpose for collection (e.g., assessment for inclusion in the cash assistance program to support new businesses);

iii) Itemised description of the use (e.g., storing on a Google file, assessing eligibility, disbursement of cash aid);

iv) Who will have access to the data and how long it will be retained;

v) Explicit consent request to Person B for the processing of her personal data.

v) If Person B expresses any concerns about sharing specific information, Z's representative must acknowledge

Actionable:

The notice provided by NGO Z to Person B must also include:

i) A disclaimer on data protection and a description of measures taken to safeguard the data;

ii) The right and process to withdraw consent, in a manner that is as easy as giving consent;

iii) Details of grievance redressal mechanisms, including whom to contact and within what timelines;

iv) The process to file a complaint with the Data Protection Board in case of unresolved grievances or misuse of data;

v) The website/app link or alternate means (such as physical address or phone number) through which Person B can withdraw her consent, and exercise her rights under the Act, such as accessing, correcting, or erasing her data.

NGO Z must also ensure that only authorised employees have access to the data strictly for defined purposes. No unrelated personnel within Z should be allowed to have access to any personal data from the database, unless required for a specific purpose.

MODEL NOTICE

[Data Principal to be given option to access contents of notice in English or any language specified in the Eighth Schedule to the Constitution]

1. Purpose of this Notice

This notice is to inform you of how we, [Name of the Data Fiduciary], want to process your personal data, so that you may give your informed consent.

2. Personal Data Collected

Only the following personal data will be collected from you for the purposes mentioned in this notice:
(a) <example: Name>
(b) <example: Email ID>
(c) <example: Credit Card Details>
(d) <example: Address>

3. Purpose of Collection

The personal data listed above will be used for the following purposes:
(a) <Name> and <Email ID> – to <example: register you as a customer>
(b) <Credit card details> – to <example: receive payments>
(c) <Address> – to <example: deliver goods>

We will only collect as much personal data as is necessary for the above purposes.
The personal data will not be used for any other purpose.

4. Retention of Personal Data

We will process your personal data only till the purposes mentioned are served:
(a) <Name> and <Email ID> – retained till <example: you remain our customer>
(b) <Credit card details> – retained till <example: payment is received>
(c) <Address> – retained till <example: goods are delivered>

5. Right to Withdraw Consent

You can withdraw your consent for processing your personal data at any time by:
<example: clicking here [hyperlink]>
Upon withdrawal, your personal data will be erased unless we are legally required to retain it.

6. Contact for Questions

If you have any questions regarding the processing of your data, you can contact us at:
<example: clicking here [hyperlink for contacting the person who will respond]>

7. Your Rights

You have the right to:
(a) Access information about your personal data
(b) Correct and update your personal data
(c) Erase your personal data
(d) Seek redress of any grievance regarding processing of your personal data
(e) Nominate someone to exercise these rights in case of death or incapacity

8. Grievance Redressal and Other Rights

You can:
- Register any grievance by <example: clicking here [hyperlink]>
- Exercise other rights by <example: using the same link>

If no reply is received within <example: 72 hours>, you may approach the Data Protection Board of India at
<example: clicking here [hyperlink]>

9. Save or Download Notice

You can save a copy of this notice by:
<example: clicking here [hyperlink]> and download it on your mobile.

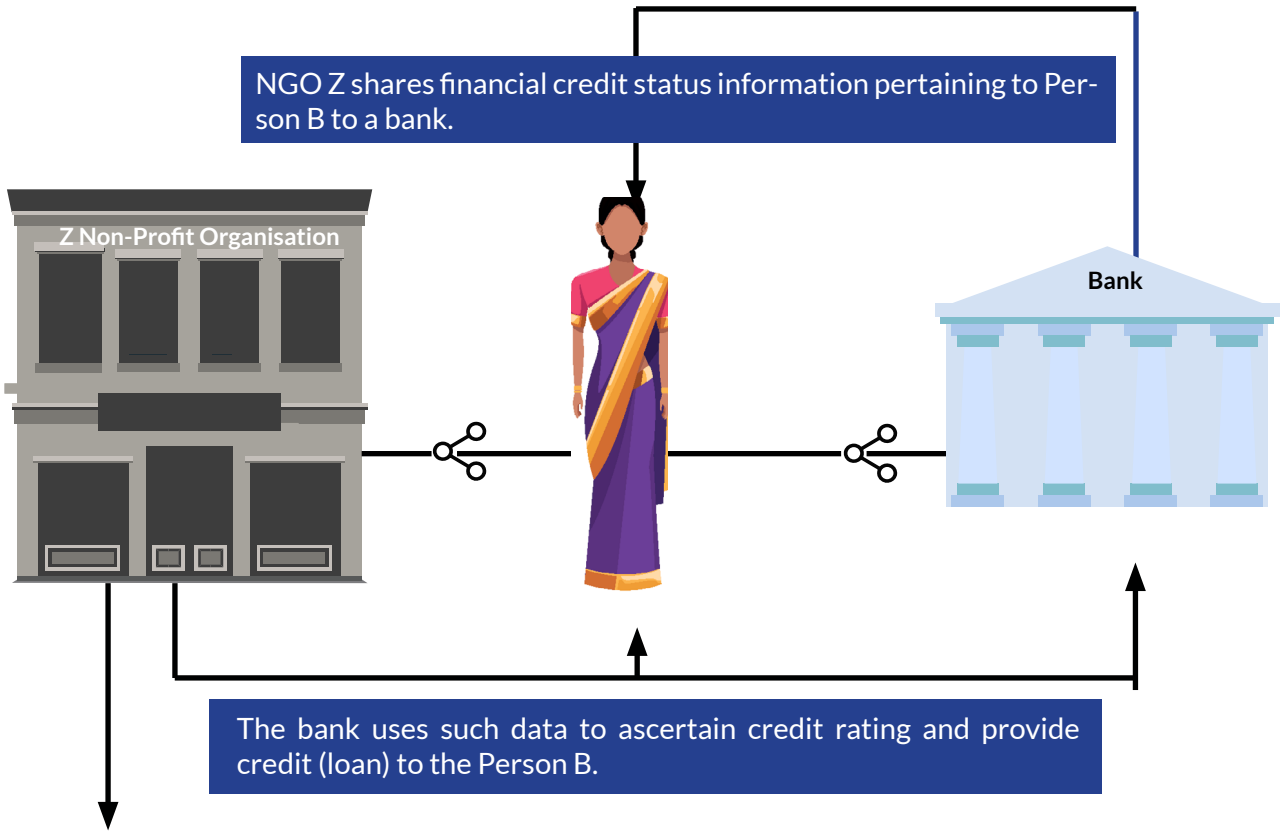
Section 6 - Data Fiduciary's Obligations under the Act

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:2

Ensuring Data Accuracy: Key Obligations for NGOs



Implications:

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

ii. Security Measures:

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

Protection of personal data can be through methods such as encryption, masking, or the use of virtual tokens. While NGOs acting as Data Processors may not be directly responsible for obtaining consent or responding to Data Principals' requests for the exercise of their rights, they are expected to operate responsibly. Such NGOs are also expected to adhere to reasonable safeguards and procedures, such as:

(a) implementing access control measures to ensure that only authorised personnel can access computer systems handling personal data.

(b) maintaining logs and monitoring systems to track data access for the purpose of detecting, investigating, and preventing unauthorised access.

(c) ensuring continuity of data processing through appropriate backup and recovery mechanisms in the event of data loss or security breaches.

(d) retaining logs and relevant data for a minimum of one year to support the detection and investigation of security incidents, unless a different period is prescribed by law.

(e) ensuring that any third party handling its data is contractually obligated to adhere to strict security safeguards.

(f) implementing necessary technical and organisational measures to preserve the confidentiality, integrity, and availability of personal data.

(g) ensuring that any contract signed with a Data Processor includes clear provisions requiring the Data Processor to take proper security measures to protect personal data. In addition, the Data Fiduciary must implement suitable technical and organisational steps to make sure these security measures are followed effectively.

iii. Notify Data Breaches :

In the event of a Data breach involving Personal Data of Data Principals, Data Fiduciaries must promptly notify the Data Protection Board 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. Further, the Data Fiduciary shall, to the best of its knowledge, promptly inform each affected Data Principal in a concise, clear, and plain manner, and without delay, using their user account or any registered mode of communication.

I. The notification to the Data Principal shall include:

(a) a description of the breach, including its nature, extent, timing, and location of occurrence;
(b) the consequences relevant to the Data Principal that are likely to arise from the breach;
(c) the measures implemented and being implemented by the Data Fiduciary to mitigate the risk;
(d) the safety measures that the Data Principal may take to protect their interests; and
(e) the business contact information of a person authorised to respond to any queries on behalf of the Data Fiduciary.

II. The Data Fiduciary shall, without delay, intimate the Data Protection Board of such breach, providing:

(a) a description of the breach, including its nature, extent, timing, and location of occurrence; and
(b) the likely impact of the breach.
(c) Further, within seventy-two hours of becoming aware of the breach, or within such longer period as may be allowed by the Board upon written request, the Data Fiduciary shall submit to the Board:

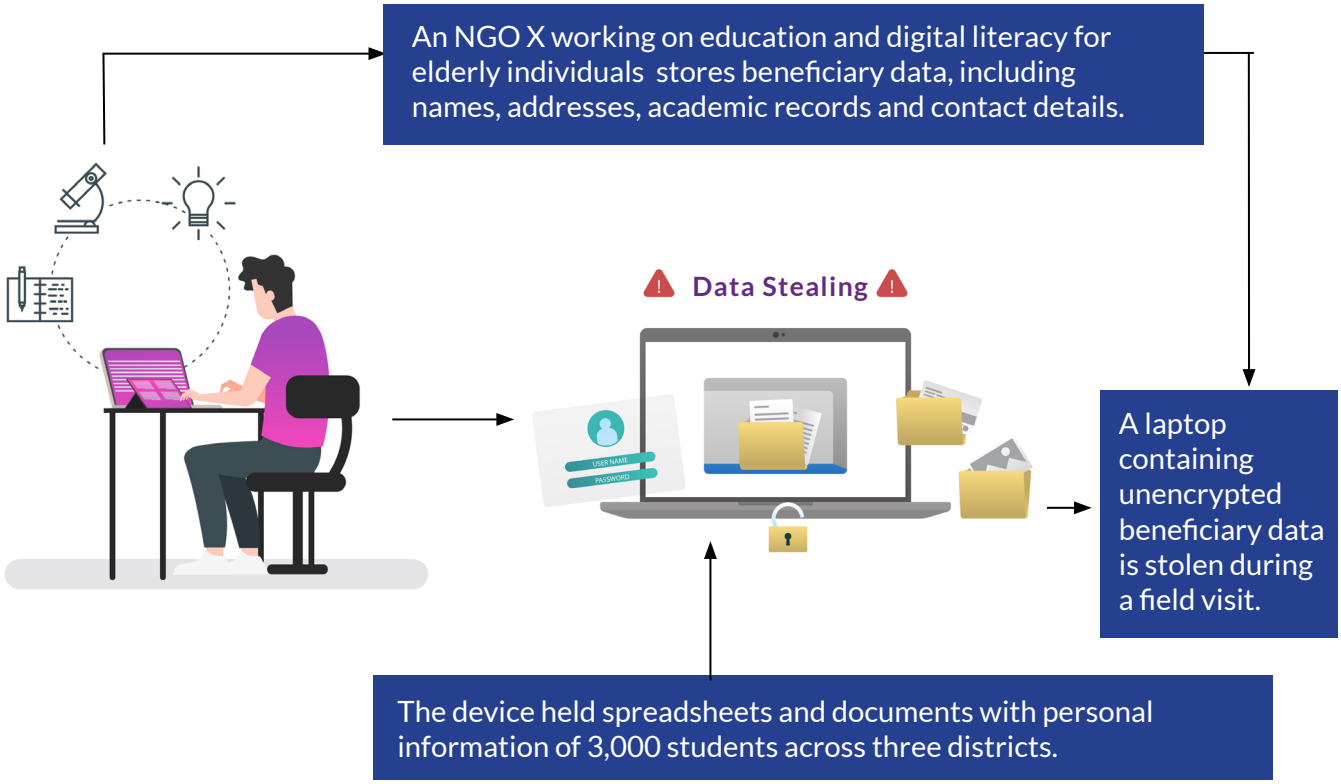
(i) updated and detailed information regarding the breach;
(ii) the broad facts related to the events, circumstances, and reasons leading to the breach;
(iii) the measures implemented or proposed to mitigate the risk;
(iv) any findings regarding the person responsible for causing the breach, if available;
(v) remedial measures taken to prevent recurrence;

III. Data Protection Officer or any designated Point of Contact must mandatorily report the incident to CERT-In immediately upon becoming aware of it, following the method and format specified on the CERT-In website.

IV. The Data Fiduciary is also required to maintain logs of all their Information and Communications Technology (ICT) systems for a rolling period of 180 days, which must be provided to CERT-In either along with the incident report or upon direction from CERT-In.

Illustration 3

Data Breach: Responsibilities and Response Plan



Implications:

- The NGO is required to notify both the Data Protection Board and the affected individuals (or their guardians) as soon as it becomes aware of the breach.
- The information provided to affected individuals must be clear, concise, and in plain language.

Actionables for the NGO

Before a Breach: Preventive Measures

- Assign a person responsible for data protection.
- Ensure that only authorised personnel have access to personal data.
- Encrypt files and use secure devices for storing and transporting data.
- Train staff on data handling and breach protocols.
- Create an internal data breach response plan.

After a Breach: Immediate Response

- Notify the Data Protection Board without delay, including:
  - A description of the breach (nature, extent, timing, and location).
  - The likely impact on affected individuals.
- Within seventy-two hours (or within an extended time if permitted), submit to the Data Protection Board:
  - Detailed facts and circumstances of the breach.
  - Information on actions taken to reduce risks.
  - Any findings on the cause or responsible party.
  - Preventive steps for future breaches.
  - A summary of how and when individuals were informed.

Additionally, the DPO or designated contact must promptly report incidents to CERT-In as per its prescribed format. NGO X must retain ICT system logs for 180 days and share them with CERT-In when required.

- Notify affected individuals (or their guardians) promptly, clearly stating:
  - What happened and when.
  - What it means for them.
  - How they can safeguard their interests.
  - What steps the NGO X is taking in response.
  - Who they can contact within the NGO X for further information.

- **Long-Term Response**
  - Review and revise existing data protection measures.
  - Improve internal policies and staff training.
  - Maintain documentation of the breach and the steps taken.

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, under Rule 8 of the DPDP Rules, Data Fiduciaries are mandated to store the personal data they have collected, and the logs relating to the same, for a minimum period of one year. After that period of one year, the Data Fiduciaires must mandatorily delete the personal data, unless they are required to store it under any other law. In other words, any personal data stored and processed by a Data Fiduciary must be retained for one year, after which it must be deleted unless there is a mandate under another law. Notably, the Act also 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. The Data Fiduciary must notify the Data Principal at least forty-eight hours before the scheduled deletion of her personal data. This notice must inform the Data Principal that her personal data will be erased once the specified retention period ends, unless:

- Data Principal logs into her user account, or
- Data Principal contacts the Data Fiduciary to either:
  - Continue the processing for the specified purpose, or
  - Exercise her rights related to the processing of the data.

v. Appointment of a 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. Every NGO shall prominently publish on its website or app, and mention in every response to a communication for the exercise of the rights of a Data Principal under the Act, the business contact information of the Data Protection Officer, or a person who is able to answer on behalf of the NGO the questions of the Data Principal about the processing of her personal data.

vi. Grievance Redressal Mechanism:

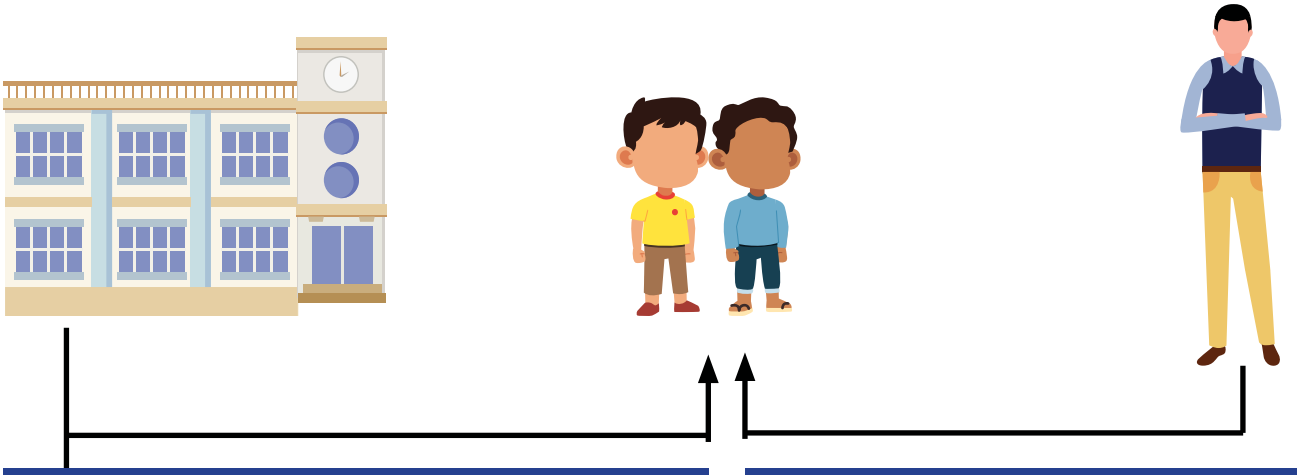
The Data Fiduciary must establish an effective mechanism to redress the grievances of Data Principals. Further Data Fiduciary must publish the period it takes to respond to grievances under its grievance redressal system. This information must be made available on its website, app, or both, as applicable.

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 4

Cross-Border Transfer of Data for Research



A non-profit 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 non-profit 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 non-profit 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 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 or monitoring children, or providing them with targeted advertisements. 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.

NGOs must take technical and organisational steps to ensure that verifiable consent is obtained before processing personal data of a child or a person with a lawful guardian.

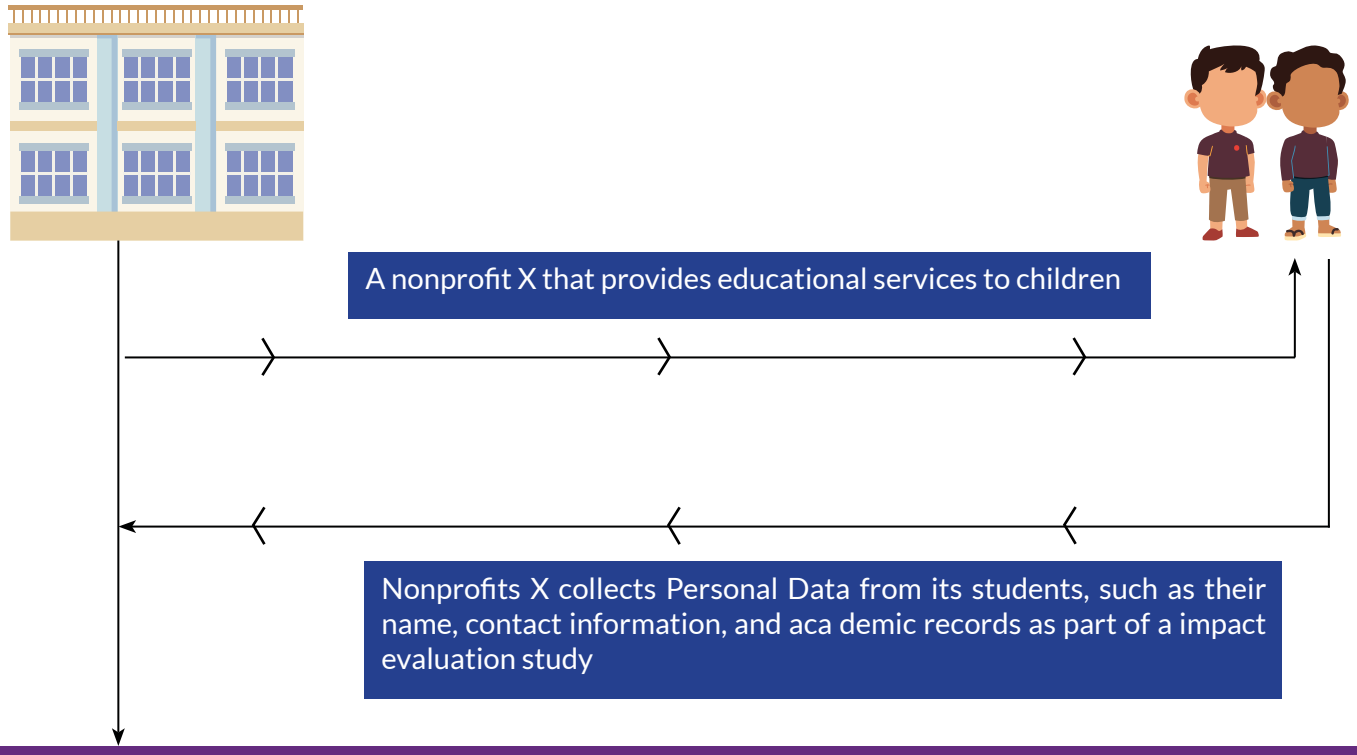
Verifiable consent must be provided by an adult who can be identified as the parent or guardian.

This identification can be confirmed through:
(a) Reliable identity and age information already available with the organisation, or
(b) Voluntarily submitted documents or virtual tokens, verified by government-authorised bodies (e.g., Digital Locker service providers).

These safeguards help ensure that consent is legitimate and traceable, reducing legal and ethical risks when working with vulnerable populations.

Illustration 5

Parental Consent and Responsibilities for NGOs in protecting Children Data



Implications:

To comply with the DPDP Act, 2023, the nonprofit must obtain verifiable parental consent before processing the personal data of its students.
This verification can be carried out through:
(a) Reliable identity and age information already available with the organisation, or
(b) Documents or virtual tokens voluntarily submitted and verified by government-authorised bodies (e.g., DigiLocker service providers).

Consent may be obtained by sharing a consent form with parents or by recording explicit parental consent within the survey form.

Data Fiduciaries are strictly prohibited from using or selling this data to target students with advertising. It must also ensure that the processing of students' personal data does not adversely affect their well-being.

These provisions impose broad and significant obligations on NGOs, especially when handling data related to children and persons with disabilities.

Section 7 - Right of the Data Principal

1. Right to withdraw consent

The Data Principal has the right to withdraw the consent she had given earlier for the collection and processing of her Personal Data. The withdrawal of consent, however, would not affect the legality of the processing of personal data before the withdrawal.

2. Right to access information about personal data

The Data Principal has the right to request and obtain from the Data Fiduciary:
i. a summary of personal data being processed and the processing activities involved.
ii. the identities of any third parties with whom the personal data has been shared, and a description of the shared data; and
iii. any other information about the personal data and its processing, as prescribed under any Applicable Law.

However, points (ii) and (iii) shall not apply when the Data Fiduciary shares personal data with third parties authorised by law to obtain such data, for purposes such as for crime prevention, investigation, or prosecution of offences or cyber incidents, based on a written request.

3. Right to correction and erasure of personal data:

i. The Data Principal has the right to correct, complete, update or erase her personal data, which she had previously consensually given, in line with Applicable Laws.
ii. The Data Fiduciary shall, upon receiving a request for correction, completion or updating from a Data Principal, —
   a. correct the inaccurate or misleading personal data;
   b. complete the incomplete personal data; and
   c. update the personal data.
iii. If a Data Principal requests the erasure of her personal data, the Data Fiduciary shall comply unless the retention of that data is necessary for a specified purpose or to comply with any Applicable Law.

4. Right to Nominate

A Data Principal shall have the right to nominate another person who, in the event of the Data Principal's death or incapacity, can exercise the Data Principal's rights under Applicable Laws.

5. Right to Grievance Redressal

A Data Principal has the right to access readily available means of grievance redressal provided by a Data Fiduciary. This right applies in cases where the Data Fiduciary has acted or failed to act in fulfilling its obligations concerning the Data Principal's Personal Data or in relation Data Principal's rights under the Act and its rules.

The Data Fiduciary is required to respond to such grievances within a prescribed period from the date of receiving the grievance.

Before approaching the Data Protection Board, the Data Principal must first exhaust the grievance redressal mechanism provided by the Data Fiduciary

Section 8 - Exemptions

The Act contains specific provisions that exempt certain types of data processing activities from the scope. These exemptions have significant implications for the rights of individuals and the obligations of Data Fiduciaries.

1. Exemption for Processing of Data for Research, Archiving, or Statistical Purposes

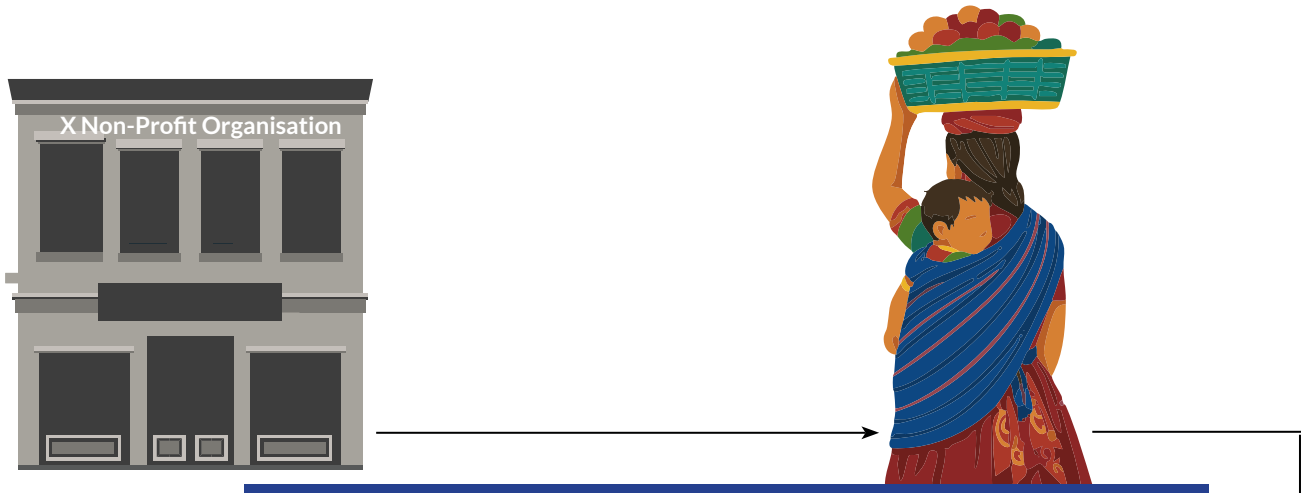
The provisions of the Act do not apply for Personal Data processed exclusively for research, archiving, or statistical purposes, under defined conditions. Archiving refers to safely storing data or records over a long period of time because such data may be useful for historical, research, or reference, and not for day-to-day use or decisions.

Conditions for Exemption:

· The processing must be necessary for research, archiving, or statistical purposes and for the intended purpose.
· The personal data must not be used to take any decision that may affect the Data Principal.
· The processing must be carried out in accordance with standards prescribed by the Government.
· The Data Fiduciary must make reasonable efforts to ensure the accuracy of the personal data.
· The Data Fiduciary must implement reasonable security safeguards to prevent personal data breaches. This includes ensuring that any Data Processor working on their behalf also follows these safeguards.
· The Data Fiduciary must share the business contact details of a person who can respond on its behalf to any questions from the Data Principal about how her personal data is being processed. It must also clearly specify the link to its website or app (or both), and describe any other available methods the Data Principal can use to exercise Data Principal's rights under the Act.

Illustration 6

Research-Based Processing of Data



Implications:

- NGO X may be exempted from provisions of the Act such as providing notice to Data Principals at the time of collection or obtaining consent for the use of their data under the Data Protection Act since the personal data is used only for research purposes.
- This exemption applies as long as:
  - The data is not used to make decisions that affect any individual participant
  - The processing is carried out following any applicable Government standards

NGO X must provide contact details of a person who can answer the Data Principal's questions about personal data processing, along with a clear link to its website or app and any other ways to exercise rights under the Act. NGO X must implement reasonable security safeguards to prevent personal data breaches.

Actionable Steps for NGO X

- **Limit Use to Research Only:** Clearly state in project documents and internal policies that the data will be used exclusively for research.
- **Avoid Individual Impact:** Ensure the data is not used to offer, deny, or alter any services for individual respondents.
- **Anonymise or De-identify Data:** Remove personally identifiable details wherever possible to reduce privacy risks.
- **Ensure Data Security:** Store data securely, control who has access, and use measures like encryption to protect it.
- **Follow Government Guidelines:** Stay updated on and comply with any standards or instructions issued by relevant authorities.

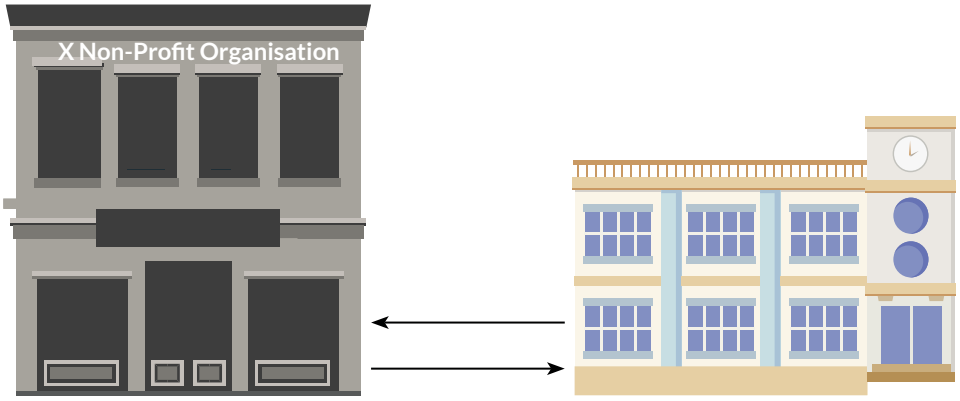
2. Verifiable Parental Consent Exceptions

Part A: Classes of Data Fiduciaries Exempted from Verifiable Parental Consent obligations

S. No	Who is exempted	When the exemption applies
1	Clinics, hospitals, mental health centres, and healthcare professionals	When they process a child's data to provide health services or advice, but only as much as needed to protect the child's health.
2	Healthcare professionals	When they support or refer a child for treatment or care, based on a health professional's recommendation, only as needed for the child's well-being.
3	Educational institutions	When they monitor children's behaviour and activities: (a) for school-related purposes; or (b) to ensure the child's safety in the school environment
4	Individuals responsible for children in crèches or day-care centres	When they monitor children's behaviour or activities to ensure their safety and well-being in these facilities.
5	Transportation staff working for schools or day-care centres	When they track a child's location during travel to and from school or a crèche, strictly for the child's safety.

Illustration 7

Exemption from Verifiable Parental Consent: Transport Safety Use Case

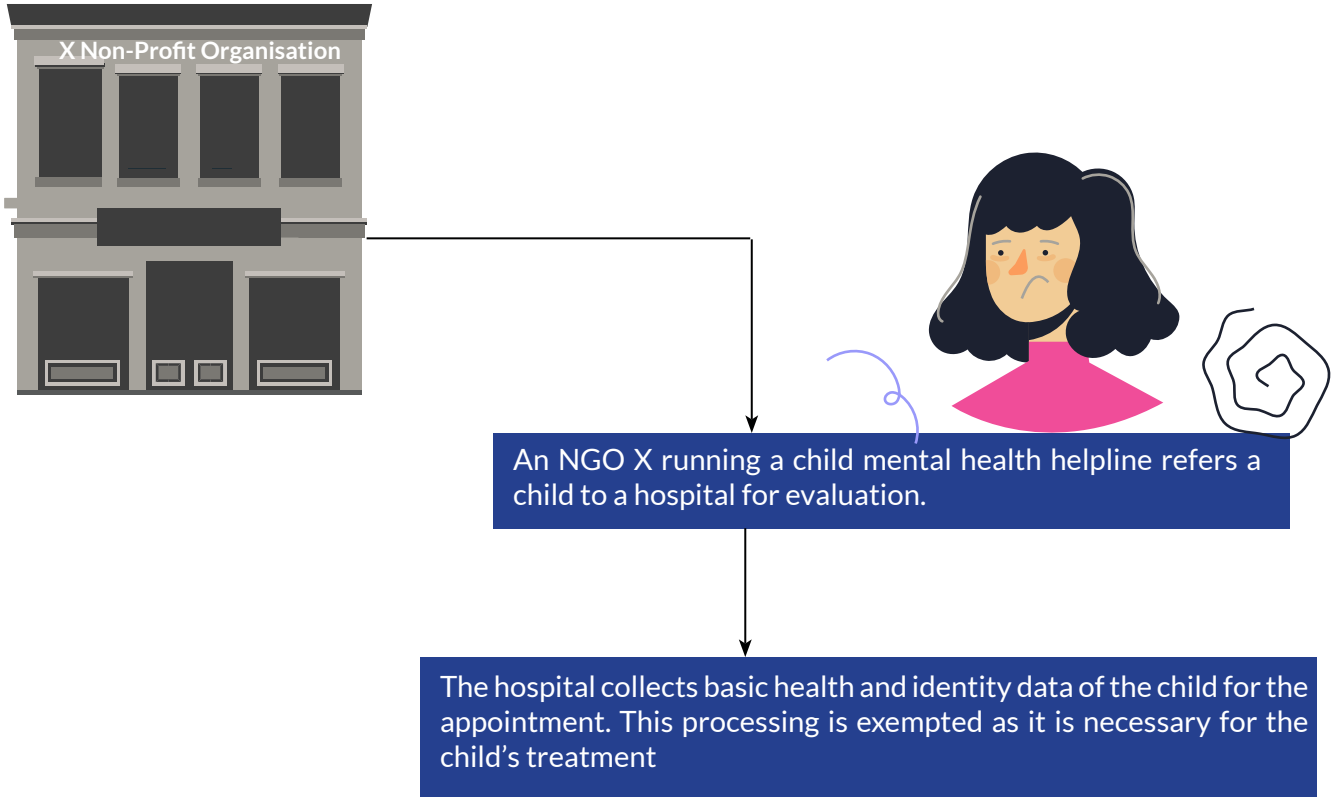


An NGO X partners with schools in tribal areas to provide transport

GPS data showing the van's route is shared with parents. The tracking of children's location during transit for safety reasons is exempted from obtaining verifiable parental consent but NGO X must implement reasonable safeguards to prevent any data breaches.

Illustration 8

Exemption from Verifiable Parental Consent: Mental Health Referral to Hospital

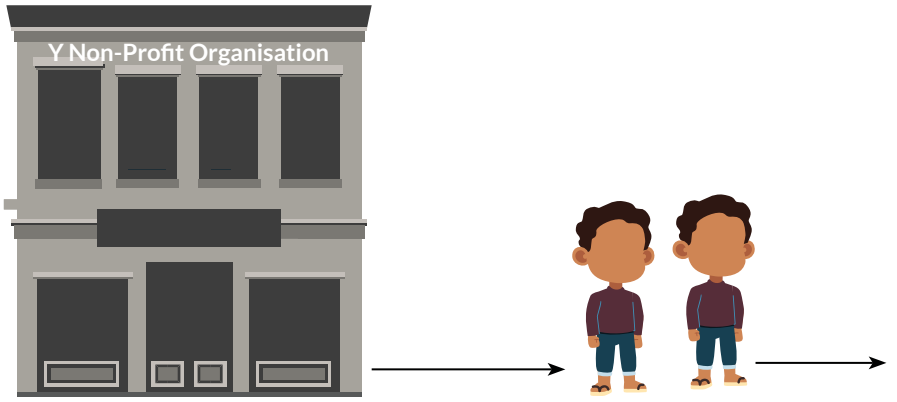


Purposes for which Verifiable Parental Consent obligations does not apply

S. No	Who is exempted	When the exemption applies
1	Exercising official duties or functions related to a child under Indian law	When processing is only done to the extent required for the specific function or duty.
2	Issuing benefits, licenses, or services (like subsidies or certificates) to a child using public funds under section	When the processing is only as much as needed to provide the benefit or service.
3	Creating a user account for a child	Only when the account is needed to communicate with the child and they cannot access the account otherwise.
4	Providing important information to the child	When the information is essential, and the child cannot receive it without the data being processed.
5	Confirming the child's age or verifying that the person giving consent is a parent or guardian	When this is necessary to meet requirements related to age or consent.

Illustration 9

Exemption from Verifiable Parental Consent: Ensuring Minimal Data Collection



NGO Y operates an educational website that provides learning materials for children.

To access the platform, children are required to create an account using basic information, including an email address.

The personal data collected is minimal and solely used to communicate with the child through the provided email address. Since the data processing is limited to what is necessary for providing access to educational content and maintaining communication, NGO Y does not have to collect Verifiable Parental Consent (VPC) but it must implement reasonable safeguards to protect children's data.

3. Permitted Purposes for Processing Personal Data

A Data Fiduciary may process the personal data of a Data Principal for the following purposes:

1. Data Principal willingly provides their Personal Data to a Data Fiduciary and has not conveyed their non-consent for the Personal Data's utilisation.
2. To provide or issue any subsidy, benefit, service, certificate, license, or permit funded by the government, where:
    a) The Data Principal has already consented to such processing, or
    b) The data is available in a government-maintained and notified database, either in digital form or digitised from a physical source.
3. For the State or its agencies to perform any legal function, or for purposes linked to sovereignty, integrity, or security of the country.
4. To comply with any legal obligation requiring disclosure of Personal Data to the State or its agencies.
5. To comply with a judgment, decree, or order, whether issued by an Indian court or related to civil or contractual claims from a foreign legal system.
6. To respond to a medical emergency, where there is a threat to the life or immediate health of the Data Principal or another person.
7. To provide medical treatment or health services during public health emergencies, such as disease outbreaks or epidemics.
8. To assist or protect individuals during disasters or situations of public disorder, as defined under the Disaster Management Act, 2005.
9. For employment-related purposes, including:
    - Safeguarding the employer from loss or liability,
    - Preventing corporate espionage,
    - Protecting trade secrets, intellectual property, or classified information,
    - Delivering employment-related services or benefits to employees.

Note: While consent and notice requirements may be exempted in the above conditions, NGOs acting as Data Fiduciaries or Data Processors must ensure that processing is conducted lawfully. They must take reasonable efforts to ensure accuracy, retain Personal Data only as long as required for the specified purpose or legal compliance, and put in place appropriate security measures to prevent personal data breaches, including during processing by third parties on their behalf.

Illustration:10

Voluntary Disclosure of Personal Data and Implied Consent

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

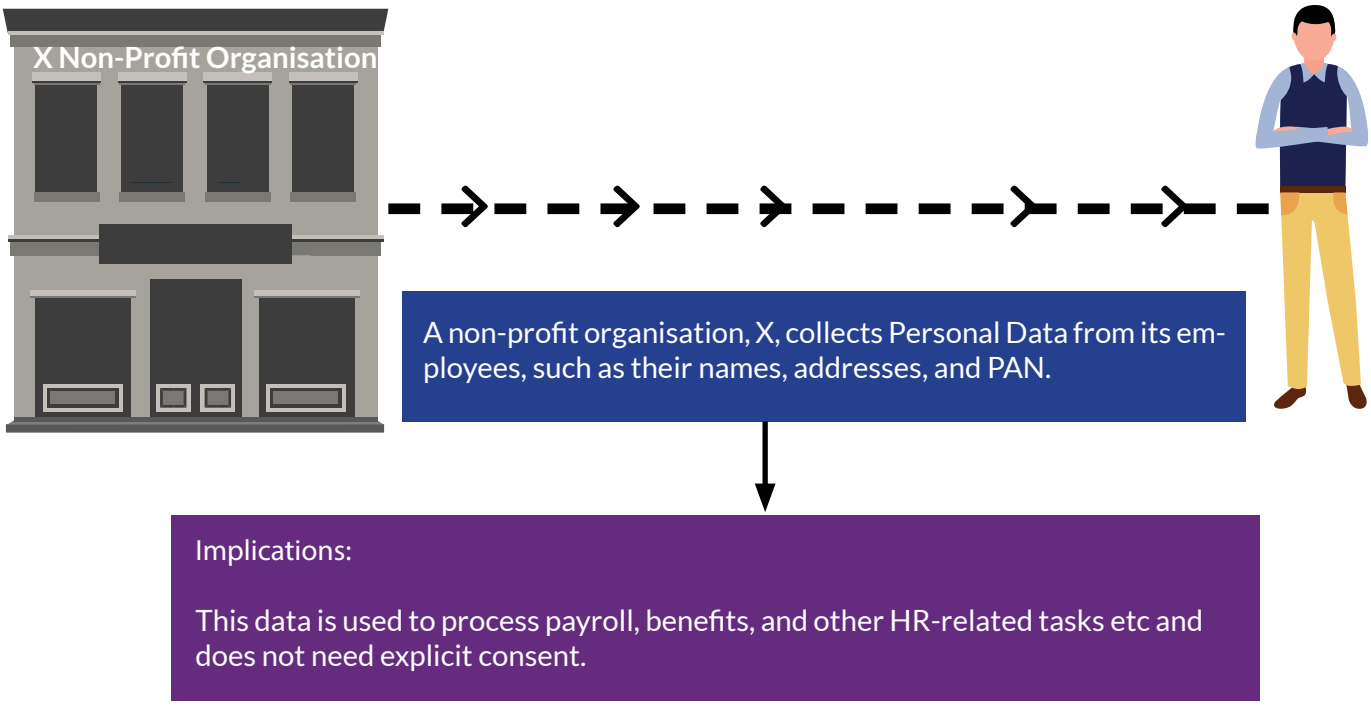
Y voluntarily provides their personal data and requests X to acknowledge receipt of the donation by sending a message to their mobile phone.

Implications:

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

Illustration:11

Employee Data Processing by NGOs



4. Processing of Health Data by NGOs under the DPDP Act, 2023

Under the act certain categories of health data processing are exempt from the requirement of collecting explicit consent. These include:

- **Public Health Initiatives :** Processing of personal health data is permitted without explicit consent when carried out for public health purposes such as vaccination drives, disease surveillance, or awareness campaigns.
- **Medical Research :** Anonymised health data may be processed for medical or scientific research, provided adequate privacy safeguards are maintained to prevent the identification of individuals.
- **Emergencies :** In situations such as pandemics, natural disasters, or other public health emergencies, health data may be processed without prior consent to ensure timely response and protection of life.

Note: Anonymisation is critical when using health data for research or statistical purposes to ensure that individuals cannot be identified, directly or indirectly.

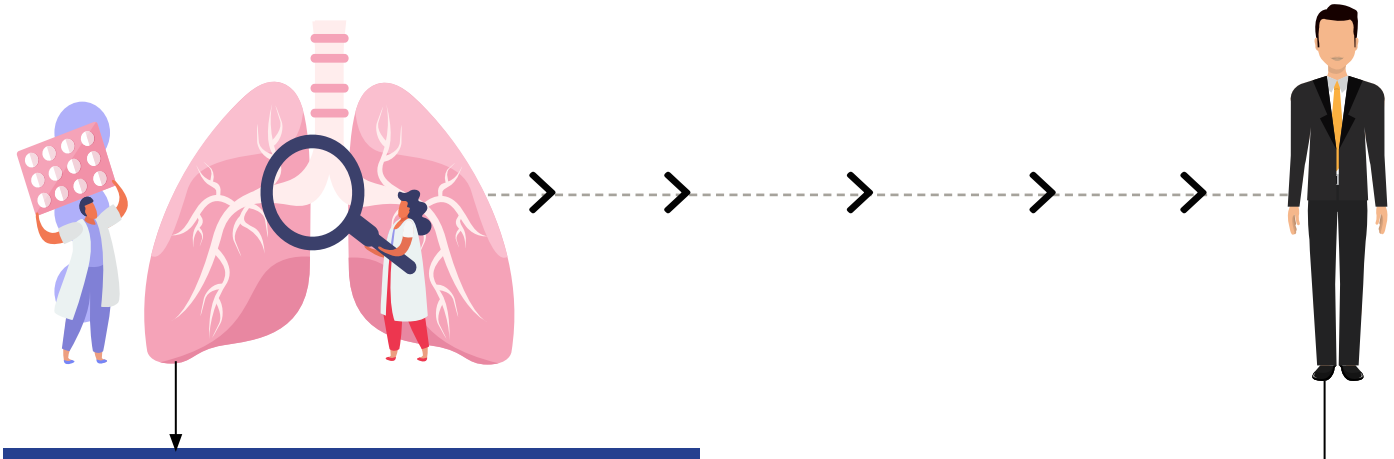
Compliance Requirements for NGOs in the Health Sector :

NGOs that process personal health data, even when exemptions apply, must adhere to the following core compliance obligations under the DPDP Act:

Obligation	Requirement
Data use Limitation	Use the data only for the specific purpose of improving public health or to respond to emergencies.
Data Security	NGOs shall implement encryption and access control mechanisms, and conduct regular audits to prevent data breaches.
Consent Management	Where consent is required, it shall be informed, specific, and revocable by the Data Principal.
Transparency	NGOs shall clearly inform individuals about the purpose of data collection and their rights under the Act.
Retention Policies	Health data shall be retained only as long as necessary for the intended purpose and securely deleted or anonymised thereafter.
Accountability	NGOs shall appoint a qualified Data Protection Officer (DPO) to oversee compliance, manage audits, and act as a point of contact with the Data Protection Board.

Illustration 12

Processing TB Health Data: Public Health Exception for NGOs



An NGO Y operates a community-based tuberculosis (TB) screening and awareness program in remote districts of India.

The initiative is conducted in partnership with district health authorities and aims to reduce TB incidence through early diagnosis, treatment linkage, and health education.

Data Processing Activities

- Collection of personal and health data (e.g., symptoms, medical history, TB test results) during field screenings.
- Anonymization of data before submitting it to public health researchers for epidemiological studies.
- Aggregation of anonymized data to identify high-risk zones and plan targeted interventions.

Applicable Exemptions

- As the program supports a government-endorsed TB control strategy, data processing is exempt from the requirement of obtaining explicit consent under the DPDP Act
- Anonymised health data shared with research institutions is exempt when adequate safeguards prevent re-identification
- During a spike in TB cases or detection of a drug-resistant strain, rapid data sharing without consent may be undertaken to support immediate response and containment

Compliance Measures Taken by the NGO:

- All data collected shall be stored in encrypted form on secure cloud servers. Field staff shall access the data through role-based login credentials. Regular audits shall be conducted to detect any unauthorised access
- For educational components or where additional data is collected beyond the public health mandate (e.g. feedback surveys), the NGO shall obtain explicit, informed consent from participants, with clear opt-out options
- Posters, pamphlets, and digital consent forms shall explain how the data will be used, stored, anonymised, and shared. Participants shall be informed of their rights under the Act, including the right to withdraw consent for non-essential processing
- Personal Data shall only be retained for the duration of the treatment cycle or project reporting timeline, whichever is longer. Post that, it shall be securely deleted or anonymised for long-term use in statistical analysis
- The NGO shall appoint a qualified Data Protection Officer (DPO) to oversee compliance, conduct regular data protection impact assessments, and liaise with the Data Protection Board if required

Section 9 - Data protection through Design : Outlawed India's Experience

DPDPA compliance begins by ensuring that the routine processes involved in any organisation's activities consider the implications of data protection and incorporate necessary safeguards. OutLawed India ("OL India"), a non-profit company working towards enabling last-mile justice delivery, has taken multiple measures to ensure that the sensitive data it collects remains protected. This Chapter seeks to examine the steps that OL India has taken, and what other organisations can emulate from their example.

The Use-Case

OL India works through a cadre of community-based paralegals – Nyaaya Mitras – who provide legal aid to various underserved communities. In practice, the work generates sensitive personal information ranging from identity documents and details of employment and income, to data on personal experiences such divorce and discrimination. This leads to a requirement to handle personal data in a safe, consistent and usable way that caters to the need of both field and central teams. Any processes and safeguards put in place had to work around operational needs: intuitive interface for Nyaaya Mitras with limited tech familiarity, ease of collection and transposition for analysis for the central team, etc. OL India decided to re-work their data collection practices by deploying a custom tool that could serve their needs. While doing so, they ensured that its design and deployment aligned with DPDP principles.

The Principles behind the Tool

The process of designing a custom tool led OL India towards the creation of a Telegram chatbot, supported by a back-end Case Management System that stores case details and allows the OL team to view and manage cases. The following section outlines some of the considerations that OL India used while designing the tool.

1. Purpose Fit: The first priority for OL India was ensuring that the tool could be used by Nyaaya Mitras and align with their existing behaviours (texting on WhatsApp) while solving challenges like fragmented data, delayed reporting, and lack of visibility into live cases.

2. Data Minimisation: The data fields to be collected were revisited to ensure minimisation: only such data that would be essential for case handling, follow-up and program accountability were retained. Nyaaya Mitras were trained to identify data relevant from a legal perspective and to upload only such data.

3. Simplified Privacy Policy and Notice: While drafting a privacy policy, the accessibility requirements of Clients and Nyaaya Mitras were prioritised to ensure simplicity. A conversational one-pager was also drafted that Nyaaya Mitras could use to explain while collecting consent from clients. Nyaaya Mitras were also encouraged to add examples and further explanations in their own languages, further improving accessibility.
4. Consent Collection: Consent collection methods were decided based on ensuring minimal additional burdens on Nyaaya Mitras. As they already listed names of individuals in a register, the OL India team designed a notebook containing a simplified explainer to the privacy policy in multiple languages, with each page having a place for signing to signify agreement with the privacy policy. The flow of data in the bot was also designed so that Nyaaya Mitras would need to upload a picture of the consent notebook before sharing details.
5. Anonymity: To ensure that clients who are unwilling to share personal details can also receive services, Nyaaya Mitras were trained to understand the importance of anonymity, and how they can anonymise details.

Our Learnings

OL India's approach highlights how ease-of-use can be balanced with data protection requirements. While their specific contexts influenced the decisions taken towards creating the final chatbot, OL India's approach is educational for all non-profit organisations working with personal data.

1. Training and Sensitisation of Staff: One of the most significant aspects of OL's approach has been the emphasis on training Nyaaya Mitras, which has ensured that each member is sensitive to the importance of data protection safeguards. By ensuring that employees and volunteers at every level are aware of the way their roles impact organisational data practices, and of the importance of data protection for their clients, organisations can minimise the potential for human error leading to data breaches.
2. Privacy-By-Design: OL India used the opportunity of creating a new data collection tool to incorporate privacy by design in their processes. Prioritising data minimisation, anonymisation and ease-of-use can reduce the probability of security incidents affecting personal data of clients.
3. Accessible Privacy Notices: DPDPA mandates that Data Principals are made aware of their rights over the data that they share. OL India has ensured that both its frontline workers and their clients can easily understand these rights by creating accessible privacy notice and consent forms in various local languages.
4. Easy Consent Collection: Collecting and recording consent for data collection is critical. By integrating consent collecting in the workflow such that frontline workers cannot upload data without collecting consent, OL India removes ambiguity and can showcase compliance.

Further Steps

All Data Fiduciaries collecting personal data need to be compliant with the mandates under DPDPA. By designing their data collection processes while incorporating privacy-by-design, organisations can ensure that they remain in compliance with the applicable mandates and protect their beneficiaries' data. Further, by putting in place technical safeguards to protect stored data, strict data retention timelines to delete unnecessary data, and appointing a Data Protection Officer, organisations can meaningfully comply with the requirements under DPDPA.

https://www.pacta.in/

https://www.linkedin.com/company/pactaindia/

@PactaIndia