PACTA
SOCIAL | IMPACT | LEGAL

Chitta
Initiative for Research by Pacta

Understanding the DPDP Act, 2023 and Draft Rules, 2025

A Primer for NGOs

Content

Chapter 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 Digital Personal Data Protection Act, 2023 (DPDP Act) was notified in the official gazette after being passed by the Parliament and receiving Presidential assent. Following its enactment, on January 3, 2025, the draft Digital Personal Data Protection (DPDP) Rules, 2025 were released for public consultation. These rules invited feedback from stakeholders across different sectors, and Pacta submitted its comments[3] during the process. The final rules are expected to be notified shortly, paving the way for phased implementation of India's data protection framework.

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 organisations 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 per sonal data or information) Rules, 2011, will govern questions of data privacy.[4]

[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://e6a1ddce-638a-4c2a-a468-3bb06cb66ec2.usrfiles.com/ugd/0e1e8f_dac3c556ab8d4ecba1026b43d60e2bbc.pdf
[4] https://www.pacta.in/blog/Data-Protection-for-Civil-Society-Organisations.htm

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

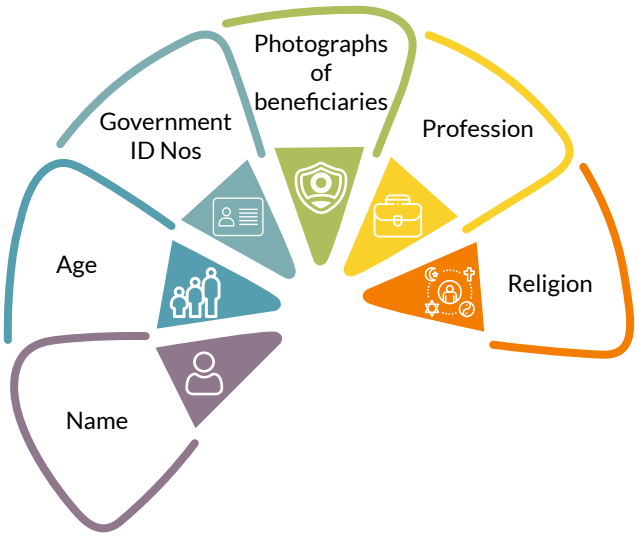
The Act will apply to the processing of Personal Data collected in India in two situations:

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

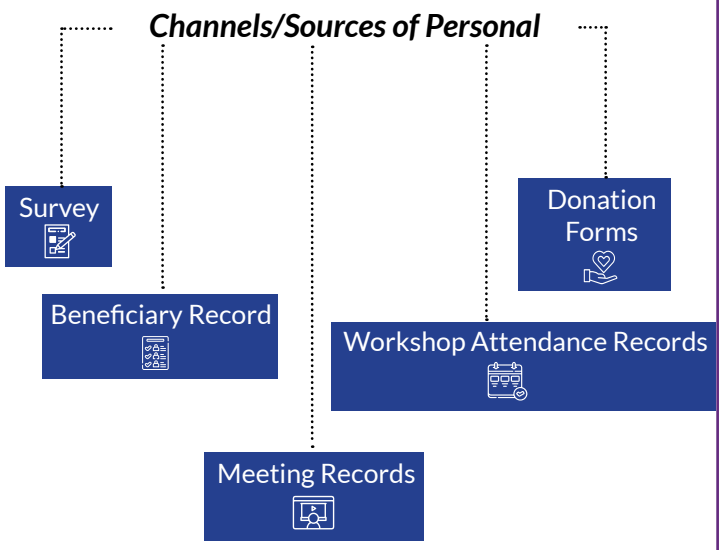
ii. when Personal Data is collected offline and then transferred to a digital format.

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



NGOs indulging in the above activities of collecting and processing of Personal Data. Thus the Act will also apply to all nonprofits and charitable organisations that collect personal information from their stakeholders online or offline and then digitise it.

Chapter 3 - Data Privacy Jargon Debunked

a. **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.

b. **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.

c. **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.

d. **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.

e. **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 would assume the role of data fiduciaries.

f. **Data Principal:** The individual to whom the personal data pertains, including a child's parents or legal guardians in cases where the data subject is a minor (under 18 years of age) or a person with a disability.

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

h. **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.

i. **Data Protection Officer (DPO) :** A mandatory appointment for Significant Data Fiduciaries. The DPO ensures internal compliance with the Act and serves as the designated point of contact for Data Principals and the Data Protection Board.

j. **Digital Office:** 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.

k. **Digital Personal Data:** It is the Personal Data in a digital format.

l. **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).

m. **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.

Chapter 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[5] 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 organisation, rather than having to comply with different rules in different countries. The Brussels Effect is often seen as a form of soft power.

India's Digital Personal Data Protection Act, 2023, reflects the influence of the GDPR and the broader Brussels Effect. It incorporates several aligned concepts, including the defined roles of Data Fiduciaries and Data Principals, lawful processing based on informed consent, and other foundational principles such as data minimisation, purpose limitation, and protection of individual rights. These similarities underscore the impact of the Brussels Effect in India's data protection regime, and how there has been an effort to align the DPDPA with global privacy strategy.

[5] WP (C) NO. 494 OF 2012

Chapter 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.

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

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

a. **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 background, can comprehend.

b. **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, notice for consent should include

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

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

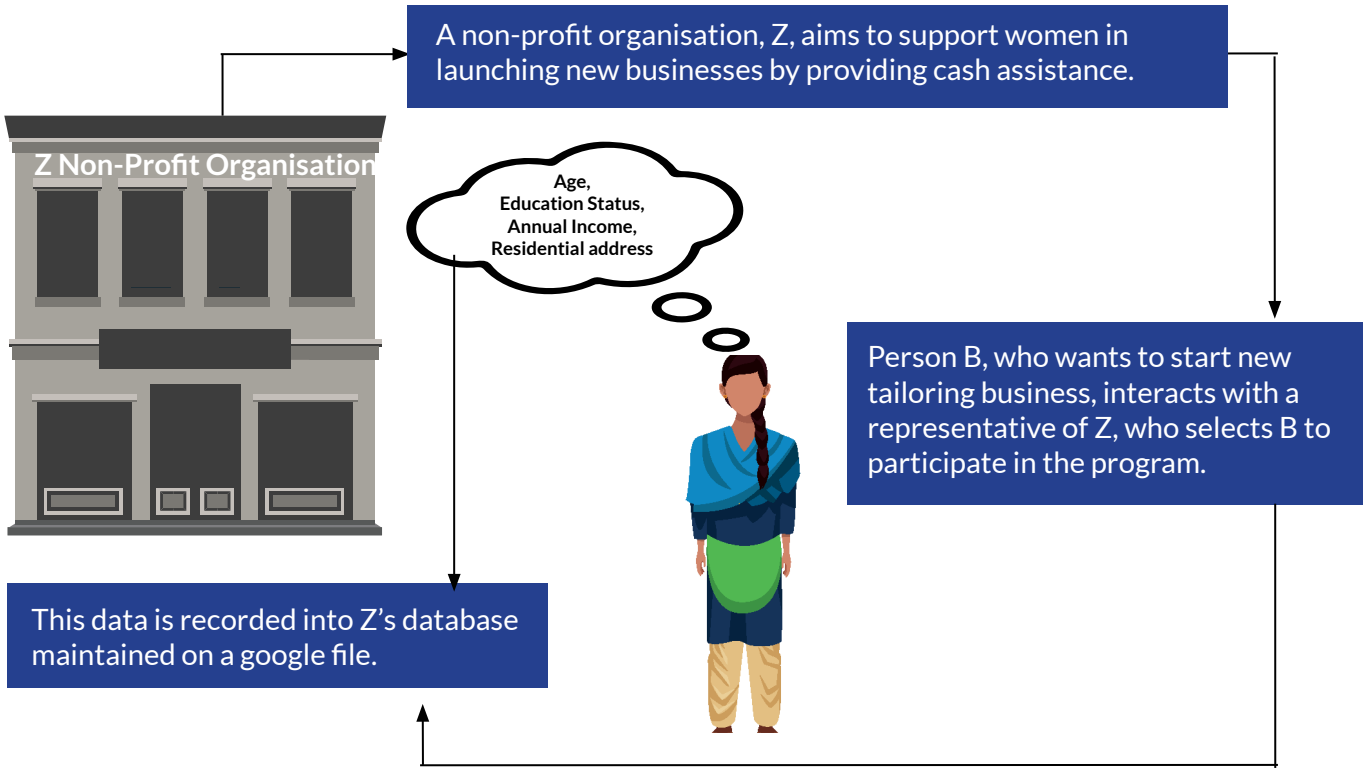
v. It should also describe means through which the Data Principal can:

   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)

Illustration1

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 from Person B for the processing of her personal data
vi. If Person B expresses any concerns about sharing specific information, Z's representative must acknowledge, address, and resolve them before proceeding further

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 are allowed 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

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

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 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

8. Grievance Redressal and Other Rights Data

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.

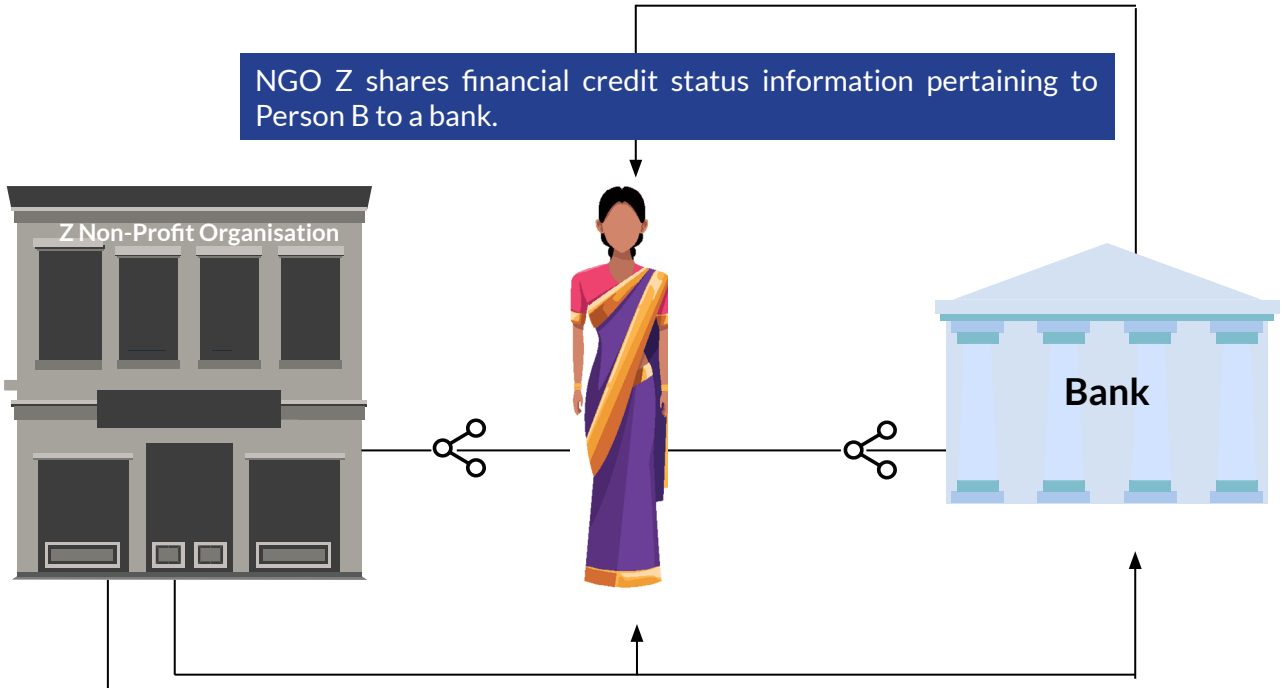
Chapter 6 - Data Fiduciary's Obligations under the Act

1. 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.

2. 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.

The Data Fiduciary shall undertake the following measures to ensure the security and integrity of personal data: The Data Fiduciary shall protect personal data 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 Principal's requests for the exercise of their rights, they are expected to operate responsibly. Such NGOs should adhere to reasonable safeguards, and procedures such as :

i. The Data Fiduciary shall implement access control measures to ensure that only authorised personnel can access computer systems handling personal data
ii. The Data Fiduciary shall maintain logs and monitoring systems to track data access for the purpose of detecting, investigating, and preventing unauthorised access
iii. The Data Fiduciary shall ensure continuity of data processing through appropriate backup and recovery mechanisms in the event of data loss or security breaches
iv. The Data Fiduciary shall retain 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
v. The Data Fiduciary shall ensure that any third party handling its data is contractually obligated to adhere to strict security safeguards
vi. The Data Fiduciary shall implement necessary technical and organisational measures to preserve the confidentiality, integrity, and availability of personal data
vii. The Data Fiduciary must ensure 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

3. Notify Data Breaches :

In the event of a Personal Data breach, Data Fiduciaries must promptly notify the Data Protection Board (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. Further, 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:

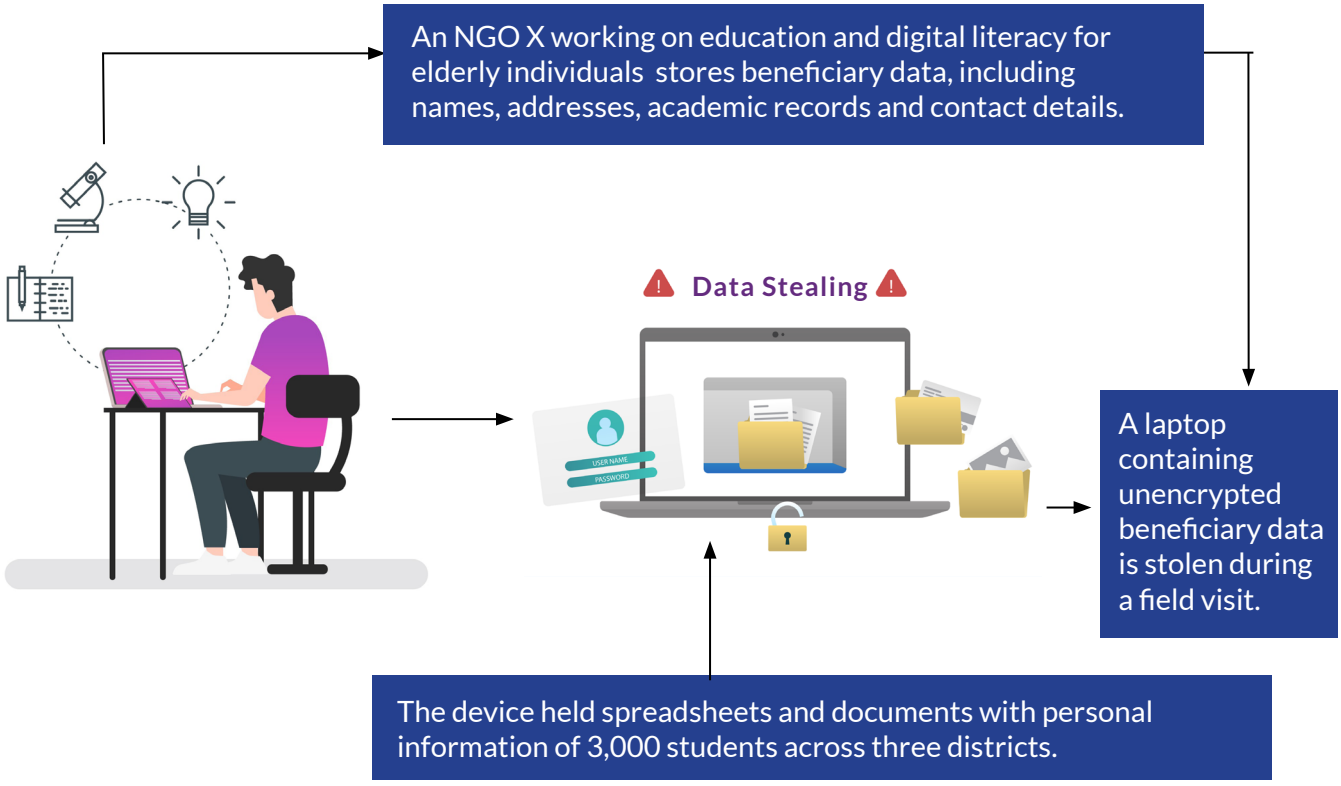
a. a description of the breach, including its nature, extent, timing, and location of occurrence and
b. the likely impact of the breach. Further, within seventy-two hours of becoming aware of the breach, or within such longer period as may be allowed by the Board upon written request, the Data Fiduciary shall submit to the Board:
   - updated and detailed information regarding the breach
   - the broad facts related to the events, circumstances, and reasons leading to the breach
   - the measures implemented or proposed to mitigate the risk
   - any findings regarding the person responsible for causing the breach, if available
   - 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



Implication:

i. 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
ii. The information provided to affected individuals must be clear, concise, and in plain language

Actionable:

Before a Breach: Preventive Measures

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

After a Breach: Immediate Response

- **Notify the Data Protection Board without delay, including:**

i. A description of the breach (nature, extent, timing, and location)
ii. The likely impact on affected individuals

- **Within seventy-two hours (or within an extended time if permitted), submit to the Data Protection Board:**

i. Detailed facts and circumstances of the breach
ii. Information on actions taken to reduce risks
iii. Any findings on the cause or responsible party
iv. Preventive steps for future breaches
v. 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:**

i. What happened and when?
ii. What it means for them?
iii. How they can safeguard their interests?
iv. What steps the NGO X is taking in response?
v. Who they can contact within the NGO X for further information?

- **Long-Term Response**

i. Review and revise existing data protection measures
ii. Improve internal policies and staff training
iii. Maintain documentation of the breach and the steps taken

4. 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. The Data Fiduciary must notify the Data Principal at least 48 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:

i. Data Principal logs into her user account, or
ii. 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

5. 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. 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.

6. Grievance Redressal Mechanism:

The Data Fiduciary shall establish an effective mechanism to redress the grievances of Data Principals. Further Data Fiduciary is required to 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.

7. 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 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.

8. 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.

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:

i. Reliable identity and age information already available with the organisation, or
ii. 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

A nonprofit X that provides educational services to children

Nonprofits X collects Personal Data from its students, such as their name, contact information, and aca demic records as part of a impact evaluation study

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).

These safeguards ensure that consent is both legitimate and traceable, thereby mitigating legal and ethical risks when working with vulnerable populations. Consent may be obtained by sharing a consent form with parents or by recording explicit parental consent within the survey form.
The nonprofit is 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.

Chapter 7 - Right of the Data Principal

1. Right to withdraw consent

The Data Principal has the right to withdraw the consent that the indivitual has given earlier for the collection and processing of their 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 their personal data, which they have 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 their personal data, 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.

4. 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.

i. The Data Fiduciary is required to respond to such grievances within a prescribed period from the date of receiving the grievance
ii. Before approaching the Data Protection Board, the Data Principal must first exhaust the grievance redressal mechanism provided by the Data Fiduciary

Chapter 8 - Exemptions

The Digital Personal Data Protection Act, 2023 (DPDPA) contains specific provisions that exempt certain types of data processing activities from the scope of the Act. These exemptions have significant implications for the rights of individuals and the obligations of data processors.

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

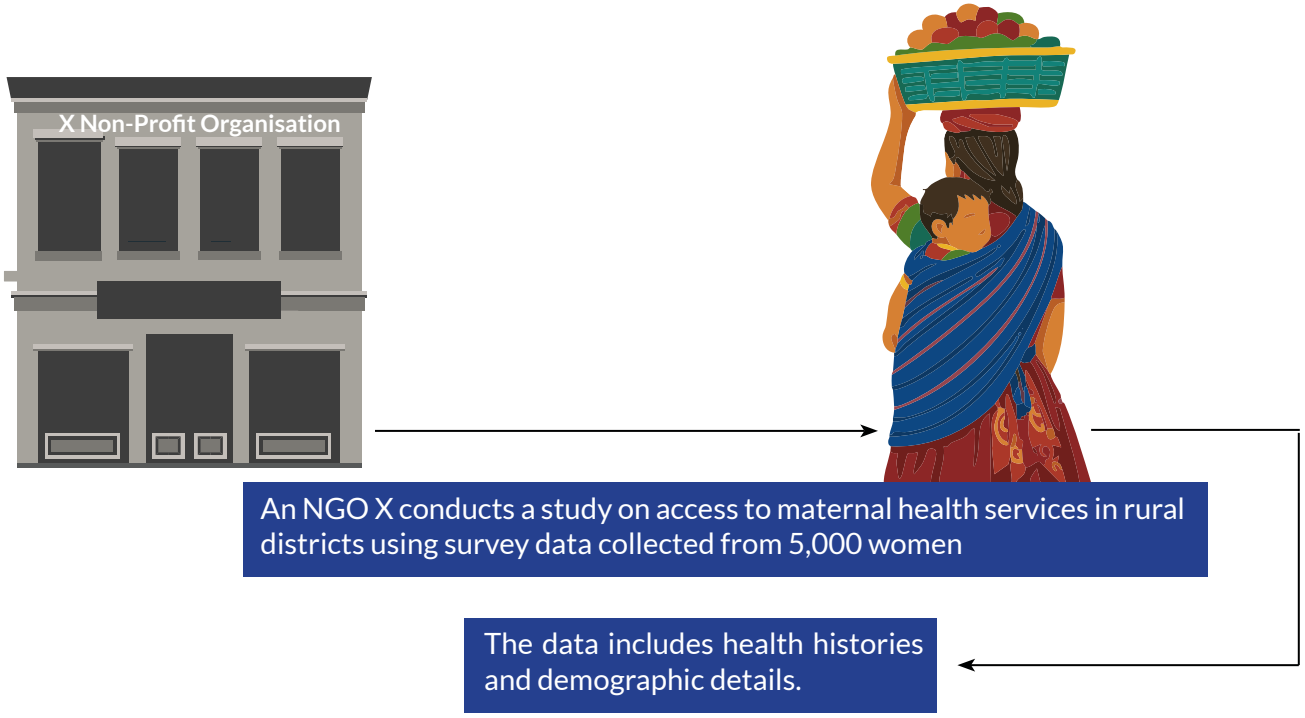
The provisions of the Act do not apply for personal data processed exclusively for research, archiving, or statistical purposes, under defined conditions. Archiving refers to safely storing data or records over a long period of time because such data nay be useful for historical research, or reference,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

Conditions for Exemption:

i. The processing must be necessary for research, archiving, or statistical purposes and for the intended purpose.
ii. The personal data must not be used to take any decision that of the Data Principal.
iii. The processing must be carried out in accordance with standards prescribed by the Government.
iv. The Data Fiduciary must make reasonable efforts to ensure the accuracy of the personal data.
v. 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.
vi. 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.
vii. The Data Fiduciary must clearly specify the link to its website or app, or both, and also describe any other available methods through which the Data Principal can exercise their 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.

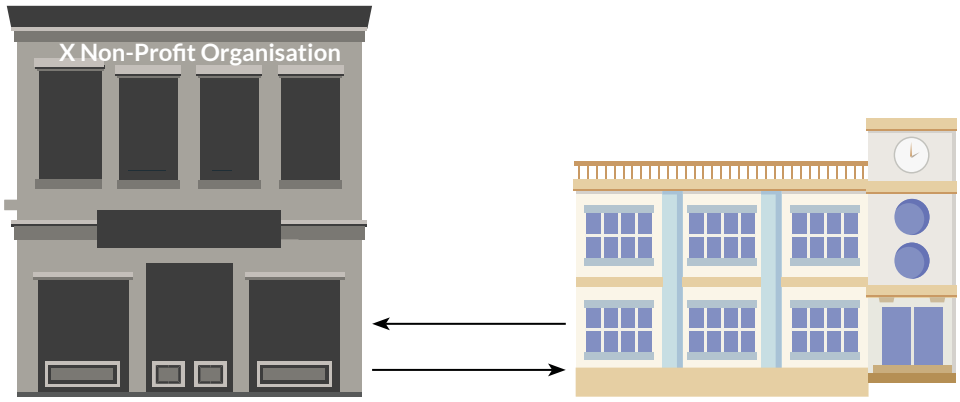
2. Verifiable Parental Consent Exceptions

i. 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 healthcare 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

An NGO X running a child mental health helpline refers a child to a hospital for evaluation.

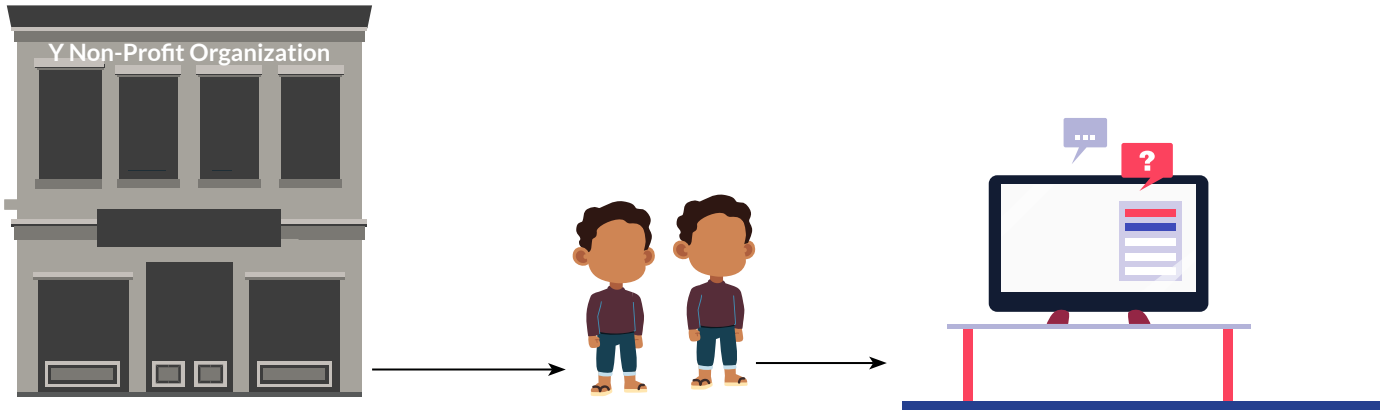
The hospital collects basic health and identity data of the child for the appointment. This processing is exempted as it is necessary for the child's treatment

ii. Purposes for which Verifiable Parental Consent obligations does not apply

S.No.	Purpose	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	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, In this case NGO Y does not have to collect Verifiable Parental Consent (VPC) but NGO Y 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:

i. Data Principal willingly provides their Personal Data to a Data Fiduciary and has not conveyed their non-consent for the Personal Data's utilisation
ii. To provide or issue any subsidy, benefit, service, certificate, license, or permit funded by the government, where:
    - The Data Principal has already consented to such processing, or
    - The data is available in a government-maintained and notified database, either in digital form or digitised from a physical source.
iii. For the State or its agencies to perform any legal function, or for purposes linked to sovereignty, integrity, or security of the country.
iv. To comply with any legal obligation requiring disclosure of personal data to the State or its agencies.
v. 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.
vi. To respond to a medical emergency, where there is a threat to the life or immediate health of the Data Principal or another person.
vii. To provide medical treatment or health services during public health emergencies, such as disease outbreaks or epidemics.
viii. To assist or protect individuals during disasters or situations of public disorder, as defined under the Disaster Management Act, 2005.
ix. 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 the above exceptions extend to the entire Act, including consent and notice requirements, NGOs acting as Data Fiduciaries or Data Processors must ensure that processing is conducted lawfully, with reasonable efforts to ensure accuracy, retained only as long as required for the specified purpose or legal compliance, and protected by 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.

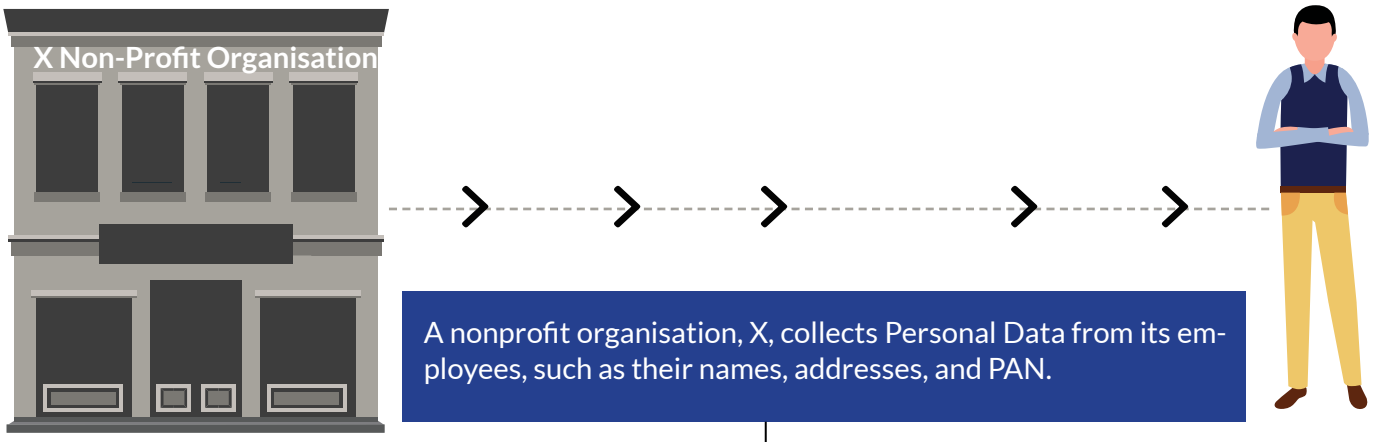
Y voluntarily provides their personal data and requests X to acknowledge receipt of the donation by sending a message to their mobile phone.

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



A nonprofit organisation, 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.

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

Under the Digital Personal Data Protection (DPDP) Act, 2023, certain categories of health data processing are exempt from the requirement of explicit consent. These include:

i. **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.
ii. **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.
iii. **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.

Although the DPDP Act provides certain exemptions, health data remains classified as Sensitive Personal Data under the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The IT Act and the SPDI Rules also impose certain obligations in line with the DPDP Act and its Rules, such as obtaining consent, allowing access and correction, restricting disclosure, and maintaining a clear privacy policy. In addition, the IT Rules recommend the implementation of reasonable security practices like ISO/IEC 27001 and the appointment of a Grievance Officer to address complaints within one month. However, once the DPDP Act and its Rules are fully notified, they will override the IT Rules.

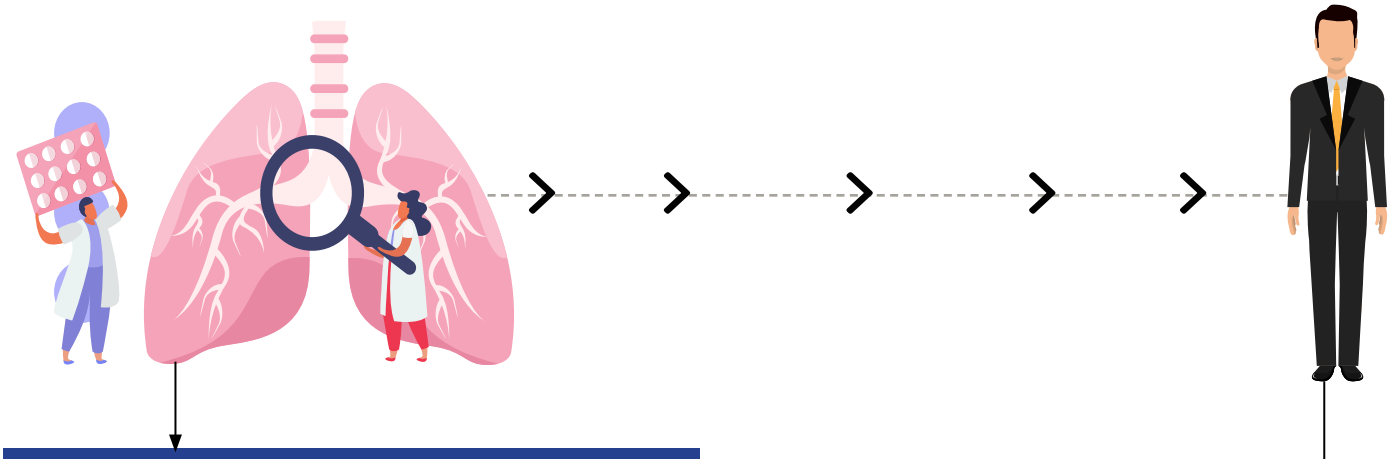
Compliance Requirements for NGOs in the Health Sector

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	The data must be used solely for the specific health purpose for which it was collected, for research purposes, or for responding to emergencies, in accordance with applicable laws and safeguards.
Data Security	NGOs shall implement encryption, access control mechanisms, and 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 DPDP 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
- Anonymisation of data before submitting it to public health researchers for epidemiological studies
- Aggregation of anonymised 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 DPDP 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

https://www.pacta.in/

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

@PactaIndia