



A PRACTICAL GUIDE

FOR CITIZENS TO
**DIGITAL PERSONAL
DATA PROTECTION ACT**



TABLE OF CONTENTS

- 03 PRIVACY GLOSSARY
- 06 INDIA'S DATA PRIVACY MOMENT
- 09 WHO DOES THE LAW APPLY TO?
- 12 WHAT IS PERSONAL DATA IN DAILY LIFE?
- 15 GIVING CONSENT THE RIGHT WAY
- 18 KNOW YOUR RIGHTS & DUTIES AS A CITIZEN
- 22 SPECIAL PROTECTION FOR CHILDREN & PERSONS WITH DISABILITIES
- 25 WHEN THE LAW DOES NOT APPLY
- 28 THE DATA PROTECTION BOARD (DPB)
- 33 PRIVACY DO'S AND DON'TS



GLOSSARY

Key Privacy Terms, Simplified



Child

Someone under the age of 18 years



Consent

Consent is defined as agreement or permission to do something, often involving authority. It signifies a voluntary agreement by someone with the capacity to choose.



Consent Manager

A Consent Manager is a person registered with the Data Protection Board who helps a citizen give, manage, review, and withdraw consent for the use of personal data through one common platform, as provided under the DPDP Act.



Data Fiduciary

An entity that decides why and how personal data is processed, either alone or with others.



Data Minimisation

Only necessary data should be collected. No excessive or unrelated data should be asked from citizens.



Data Principal

The individual to whom the personal data relates. In the case of a child or a person with a disability who is unable to act independently, this includes the parent or lawful guardian acting on their behalf.



Data Processor

A person or entity that processes personal data on behalf of a Data Fiduciary. They do not decide why the data is collected.



Digital Personal Data

Personal data that is stored, processed, or shared in digital form.



Personal Data

Any information that can identify you, directly or indirectly.



Personal Data Breach

Any unauthorised access, disclosure, loss, or misuse of personal data.



Person with Disability

A 'Person with Disability' includes individuals with long-term physical, mental, intellectual, or sensory impairments, including persons with autism, cerebral palsy, mental retardation, or multiple disabilities, who are unable to make legally binding decisions, and in some cases, even with support.



Purpose Limitation

Your data must be used only for the purpose for which it was collected. It cannot be reused for unrelated reasons.



Withdrawal of Consent

Your right to take back consent at any time. Once withdrawn, the Data Fiduciary must stop processing your data unless required by law.

Disclaimer:

The definitions are based on common understanding and not on the DPDP Act or its Rules

INTRODUCTION

This guide has been created to help citizens learn about the fundamentals of Digital Personal Data Protection framework [Digital Personal Data Protection Act, 2023 (DPDPA) and Digital Personal Data Protection Rules, 2025 (DPDP Rules)] in simple and easy to understand manner. As you move through the sections, you will gain a practical understanding of how personal data is defined and used in everyday life, and when consent must be requested, given, or withdrawn. You will learn to recognize misuse, over-collection, and unnecessary retention of personal data, and understand what you can reasonably expect from organisations that collect or process your information. The guide equips you to exercise your rights under India's DPDP Act, including knowing what steps to take if your data is misused or compromised.

Special focus is given to protecting children's data, persons with disabilities and supporting responsible digital behaviour within families. Along the way, the guide also introduces simple, everyday digital safety habits that help turn legal awareness into meaningful action.

By the end of this guide, you will not only know your rights and duties, but you will also know how to use them.

*This is not a legal handbook. This is not meant to overwhelm you with sections or clauses.
This is a Privacy Guide created to empower citizens with knowledge and awareness.*

*To read the complete details as specified under the DPDP Act and the DPDP Rules, visit:
www.meity.gov.in/static/uploads/2024/06/2b1f0e9f04e6fb4f8fef35e82c42aa5.pdf
www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf*

INDIA'S DATA PRIVACY MOMENT



INDIA NOW HAS A DATA PROTECTION LAW AND IT MATTERS TO EVERYONE

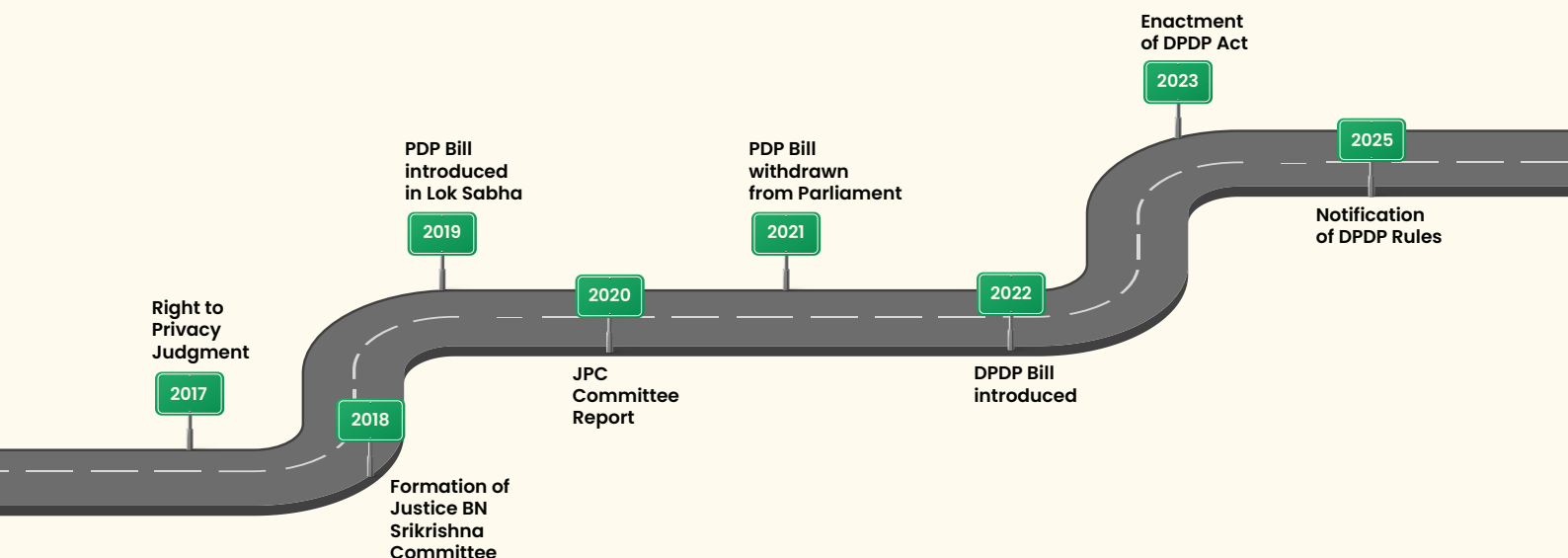
India has entered a new phase of its digital journey. With the rapid growth of digitisation across different spheres of life and online services, personal data has become a part of everyday life. Recognizing the growing role of personal data in everyday digital life, India enacted the DPDPA, supported by detailed rules notified in 2025.

The enactment of the DPDPA marked a clear shift by formally recognising privacy as a protected right.

This paradigm shift was strengthened in 2025, when detailed rules were notified to operationalise the law, translating principles into actionable obligations for organisations and enforceable rights for citizens.

The Ministry of Electronics and Information Technology (MeitY), GoI notified the DPDP Rules on November 13th, 2025. The rules were framed under the DPDPA and are now operationalising India's first data governance legislation in a phased manner.

INDIA'S DATA PROTECTION JOURNEY TIMELINE



WHAT THIS MEANS FOR CITIZENS?

Privacy is no longer a distant legal concept. It shows up in everyday moments often without us noticing. It affects:



WHAT

information is being requested from us?



WHY

it is being collected?



HOW

securely is it being stored?



CAN

we question, access, or stop its misuse?

Every click, form, app download, and consent screen involves personal data.

The DPDPA applies whenever personal data is collected, stored, used, or shared in digital form, including offline data that is later digitised. It even applies to entities not established in India, but offering goods and services to Indian citizens.

WHAT THIS CHANGE MEANS FOR CITIZENS?

- * Your personal data cannot be collected without a lawful reason.
- * You have the right to know, decide, and question.
- * Organisations must be transparent and accountable.
- * There are clear remedies if something goes wrong.



Privacy is no longer something that depends on goodwill. It is your right.

WHO DOES THE LAW APPLY TO?



WHO COLLECTS AND PROCESSES YOUR PERSONAL DATA?

In India, any legal person that collects your personal data in digital form or collects it on paper and later stores or processes it digitally. It also applies to entities not established in India, but offering goods and services to Indian citizens.

For example, some of these entities can be:



Government department and public authorities



Banks, financial institutions, and fintech platforms



Telecom and internet service providers



Hospitals, clinics, schools, and universities



Apps, websites, and social media platforms



Local businesses that collect customer details

The law applies, even if data is collected on paper but later entered into a computer system.

WHAT THIS MEANS FOR CITIZENS?

- * Your data is collected fairly and securely
- * You are clearly told why your data is needed
- * Your consent is taken without pressure
- * Misuse of your data can be questioned and penalised
- * Your data is used only for the stated purpose

Remember, as a citizen, you are no longer required to blindly trust how your data is handled. You have the right to transparency, accountability, and fairness at every stage of data processing. Organisations must justify why your data is required, ensure it is protected against misuse or breaches, and stop using it once the stated purpose is fulfilled.

Most importantly, the law empowers you to question, challenge, and seek redress if your personal data is mishandled.



If an organisation creates value out of your data, it carries a legal duty to safeguard it, respect your choices, and uphold your rights.

WHAT IS PERSONAL DATA?



UNDERSTANDING PERSONAL DATA BEYOND DEFINITIONS

WHAT IS PERSONAL DATA?

Personal data is any information that can identify a person, directly or indirectly. This may seem obvious, but in daily life, personal data often hides in plain sight.

Common examples of personal data include:



Name, phone number, email ID



Aadhaar, PAN, voter ID, passport



Photos, videos, voice recordings



Location data, IP address, device IDs



Bank details, transaction records, health records

WHAT IS SENSITIVE DATA?

Do you know, that some personal data can be sensitive in nature, and you should be extra cautious while sharing this data as any misuse, abuse, leak, or breach of such data may cause you serious harms.

Some examples of this personal data are:



Health records: Medical history, prescriptions, diagnostic reports, mental health information, vaccination details.



Financial details: Bank account numbers, credit/debit card details, UPI IDs, transaction history, income information.



Biometrics: Fingerprints, facial recognition data, iris scans, voice samples.



Identity documents: Aadhaar number, PAN, passport, voter ID, driving licence.

WHERE DO PEOPLE SHARE DATA WITHOUT REALISING?



Online & Mobile Use

- * Filling online forms (registrations, surveys, feedback)
- * Using free apps, games, or trial services
- * Signing in using social media or email accounts
- * Granting app permissions without review
- * Auto-syncing contacts, photos, or location data



Everyday Digital Transactions

- * Online shopping and food delivery platforms
- * Digital payments, wallets, and UPI apps
- * Loyalty programs, memberships, and subscriptions
- * Booking travel, events, or appointments



Social Media & Communication

- * Posting photos, videos, or location tags
- * Participating in online contests, polls, or giveaways
- * Clicking on links shared over email, SMS, or messaging apps
- * Joining groups, forums, or community platforms



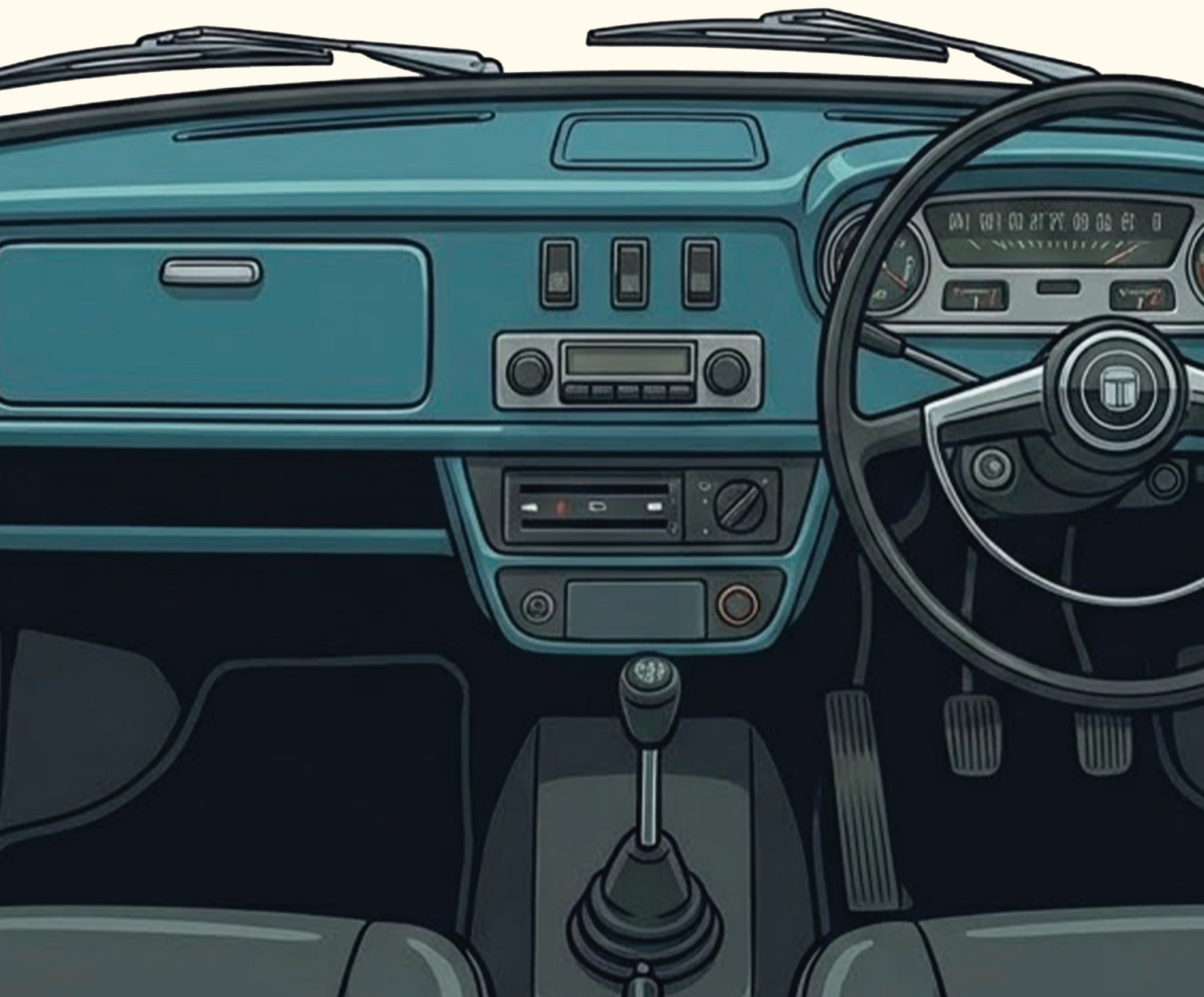
Work, Education & Health

- * Using workplace tools, attendance apps, or HR portals
- * School and college admissions and learning platforms
- * Telemedicine apps and online health records
- * Fitness trackers and wellness apps



How often do you share personal data out of habit, urgency, or convenience, without reading or questioning?

GIVING CONSENT THE RIGHT WAY



WHAT GIVING CONSENT REALLY MEANS?

Every time you download an app, sign up for a service, or tick an “I Agree” box, you are giving consent. But consent is not meant to be automatic or forced. Under DPDP Act, consent must be meaningful, given with understanding, choice, and control. This section helps you recognise what valid consent looks like in everyday situations, and how to avoid permissions that go beyond what is necessary.

WHAT DOES CONSENT REALLY MEAN?

Consent means you knowingly and freely allow an entity to collect and use your data for a stated purpose, based on the notice you receive.

Sharing your location with a cab app for a ride is reasonable. Allowing it to track you all day is not.

VALID CONSENT MUST BE



Clear and specific



Given freely



Based on proper information



Limited to a defined purpose



Easy to withdraw



Recorded properly

CHECKLIST FOR CITIZENS

✓ Does it explain what data is being collected and for what purpose?

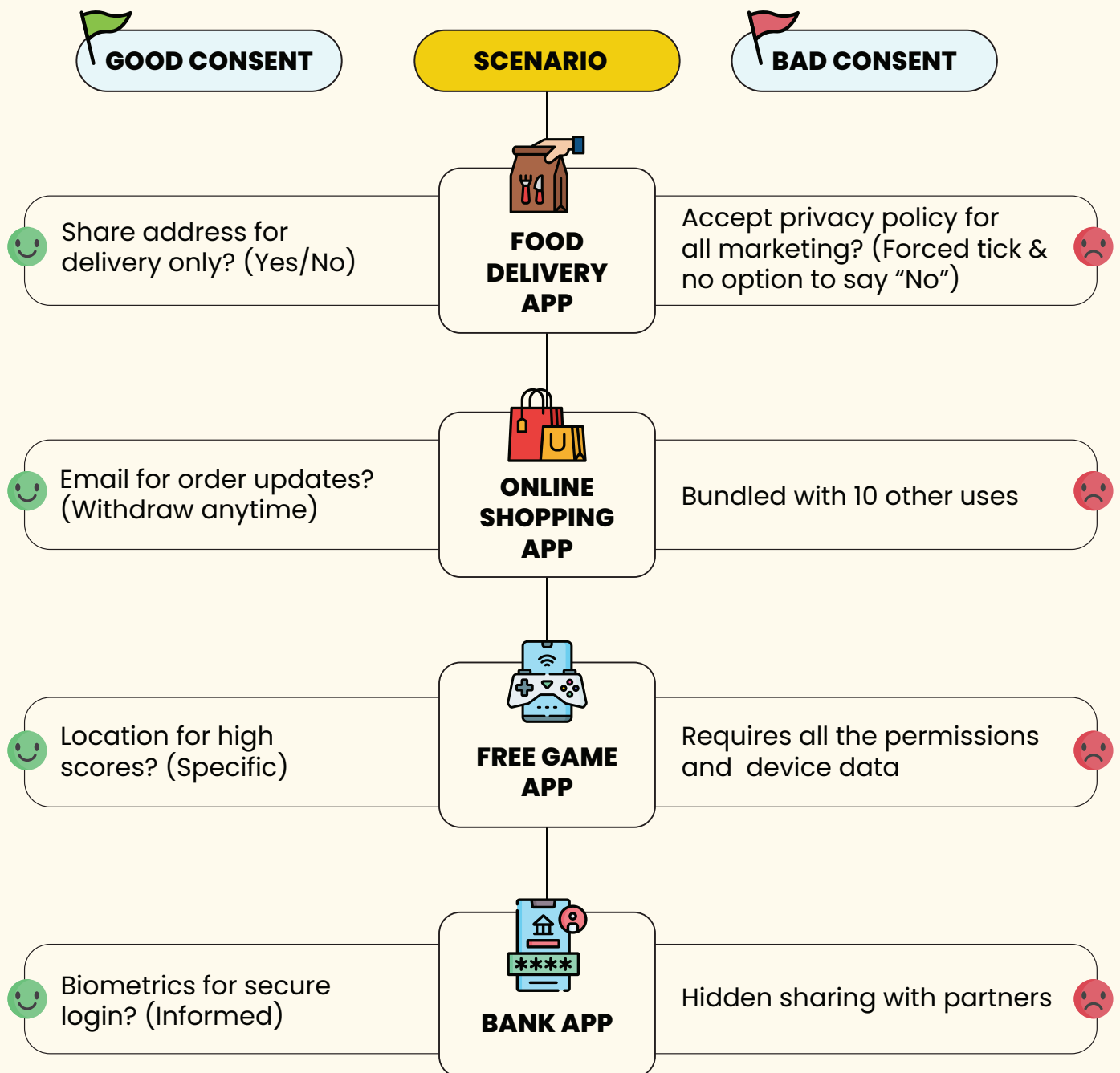
✓ Can I say no without losing service?

✓ Is withdrawal as easy as giving consent?

✓ Is the consent obtained separate for each purpose?

Ask yourself, is this consent valid?

EXAMPLES OF GREEN FLAG AND RED FLAG CONSENT HABITS



Consent must be freely given, clear, and informed. It should be given willingly, without pressure, and through a clear affirmative action. Consent must be specific to a stated purpose and limited to only the personal data necessary for that purpose.

KNOW YOUR RIGHTS & DUTIES AS A CITIZEN



UNDERSTANDING YOUR DATA RIGHTS AND DUTIES

RIGHTS THAT PUT YOU IN CONTROL OF YOUR PRIVACY



Right to Give or Refuse Consent

You have a right to allow or deny the use of your personal data for a given purpose, based on the notice given to you before your personal data is collected. You should receive notice in clear and plain language, that you understand.



Right to Know How Data is Used

You can seek information from the organisations on what personal data has been collected, why it has been collected and how it is being used. Organisations must provide this information in a simple form.



Right to Access Information about Personal Data

You have a right to access information about personal data such as summary of how it is being processed, with whom it is shared and what has been shared.



Right to Correct Personal Data

People may request corrections to personal data that is inaccurate or incomplete.



Right to Update Personal Data

Citizens can ask organizations to update their personal information when details change, such as a new address or updated contact number.



Right to Erase Personal Data

Individuals may request the removal of personal data in certain situations. The Data Fiduciary must consider and act on this request.



Right to Nominate Another Person

Every individual can also appoint someone to exercise their data rights on their behalf in the event of your death or incapacity, meaning when you are unable to take decisions for yourself.



Right to be Informed of Personal Data breach

If your personal data is breached, the Data Fiduciary must inform both the Data Protection Board and you, in the prescribed manner.



Right to Grievance Redressal

You can raise grievances with the Data Fiduciary or Consent Manager, who must resolve them within the prescribed time, and only after this can the Data Principal approach the Data Protection Board.



Right to having Personal Data kept Securely

Your Data Fiduciary must keep your personal data secure, including when it is processed by others on their behalf. To prevent data breaches, they must put reasonable security measures in place, such as:

- * Using security tools like encryption, masking, or tokenisation to protect personal data.
- * Limiting access to systems so that only authorised people can view or use personal data.
- * Continuously monitoring systems and maintaining logs to identify, investigate, and stop unauthorised access.
- * Keeping backups to ensure data can be restored if it is lost, damaged, or compromised.
- * Retaining system logs and related data for at least one year to detect, investigate, and prevent repeat security incidents, unless another law requires a different period.
- * Including security requirements in contracts with Data Processors to ensure they follow proper safeguards.
- * Implementing both technical and organisational controls to make sure these security measures work effectively.

DUTIES OF DATA PRINCIPAL

While the law empowers you with rights, there are also duties to follow to protect your rights under the law.

Citizens should:



Follow all applicable laws while exercising rights under the Act.



Do not impersonate someone else when providing personal data.



Do not hide or give false information when sharing identity or address details.



Do not raise false, misleading, or frivolous complaints or grievances.



Provide only correct and verifiable information when requesting correction or deletion of personal data.

Non-compliance with these duties may invite Penalty of up to Rs. 10,000/- as prescribed under the DPDP Act.

DID YOU KNOW?



You can voluntarily share your personal data for a specific purpose and it can be legally processed for exactly that reason. Government bodies can use your personal data to provide subsidies, benefits, services, certificates, licences, or permits without needing fresh consent each time.



Your personal data may be processed to perform functions under Indian law or to protect the sovereignty, integrity, and security of the country.



Personal data can be disclosed when required by law, such as during investigations or legal proceedings.



Authorities can process your data to comply with court orders or lawful government directions.



Your personal data can be used in medical emergencies to protect your life and health. During epidemics, disease outbreaks, or public health threats, data can be processed to provide medical treatment and control risks.

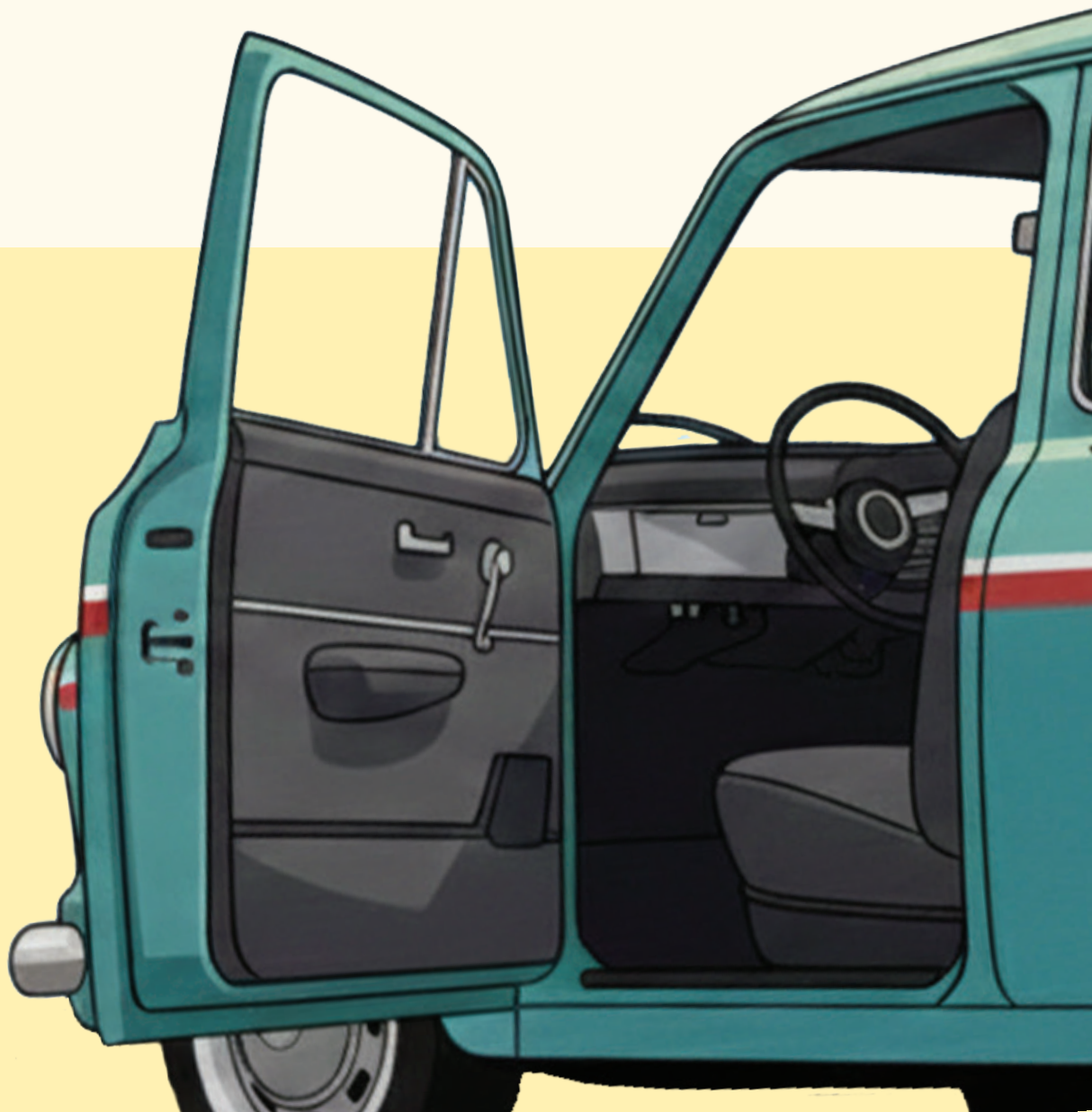


Your data may be used to provide assistance during disasters or serious breakdowns of public order.



Employers can process employee data for employment purposes including protecting the organisation from loss or legal liability.

SPECIAL PROTECTION FOR CHILDREN & PERSONS WITH DISABILITIES



SPECIAL CARE WHERE IT MATTERS MOST

Children and Persons with Disabilities (PwD) interact with the digital world differently. They may not always fully understand how their personal data is collected, used, or shared or the long-term impact it can have on their safety and well-being.

Recognising this, India's data protection law places stronger safeguards on how their personal data is handled. These protections are designed to prevent harm, misuse, and exploitation, while ensuring inclusion and accessibility.

WHAT THE LAW REQUIRES?



To collect or process a child/PwD's personal data, entities must obtain clear and verifiable consent from a Parent or lawful guardian, as applicable (for children) or legal guardian (for persons with disabilities).



A child's personal data cannot be used for tracking, behavioural monitoring, or targeted advertising.



A child's data must never be processed in ways that could harm their safety, mental health, or emotional well-being. This includes practices that may lead to exposure to inappropriate content, undue pressure, or digital addiction.

WHAT THIS MEANS FOR CITIZENS AND FAMILIES?



Parents and guardians have a key role in protecting children's digital privacy.



Persons with disabilities are entitled to equal protection and clear communication.



If something feels unsafe, misleading, or exploitative, it can and should be questioned or reported.



Certain Data Fiduciaries are not required to obtain verifiable parental consent, and the restriction on tracking or behavioural monitoring of children does not apply to them:

- * Hospitals, clinics, mental health establishments, and healthcare professionals
- * Allied healthcare professionals
- * Educational institutions
- * Individuals running crèches or child day-care centres
- * Transport providers engaged by schools or child-care centres for children

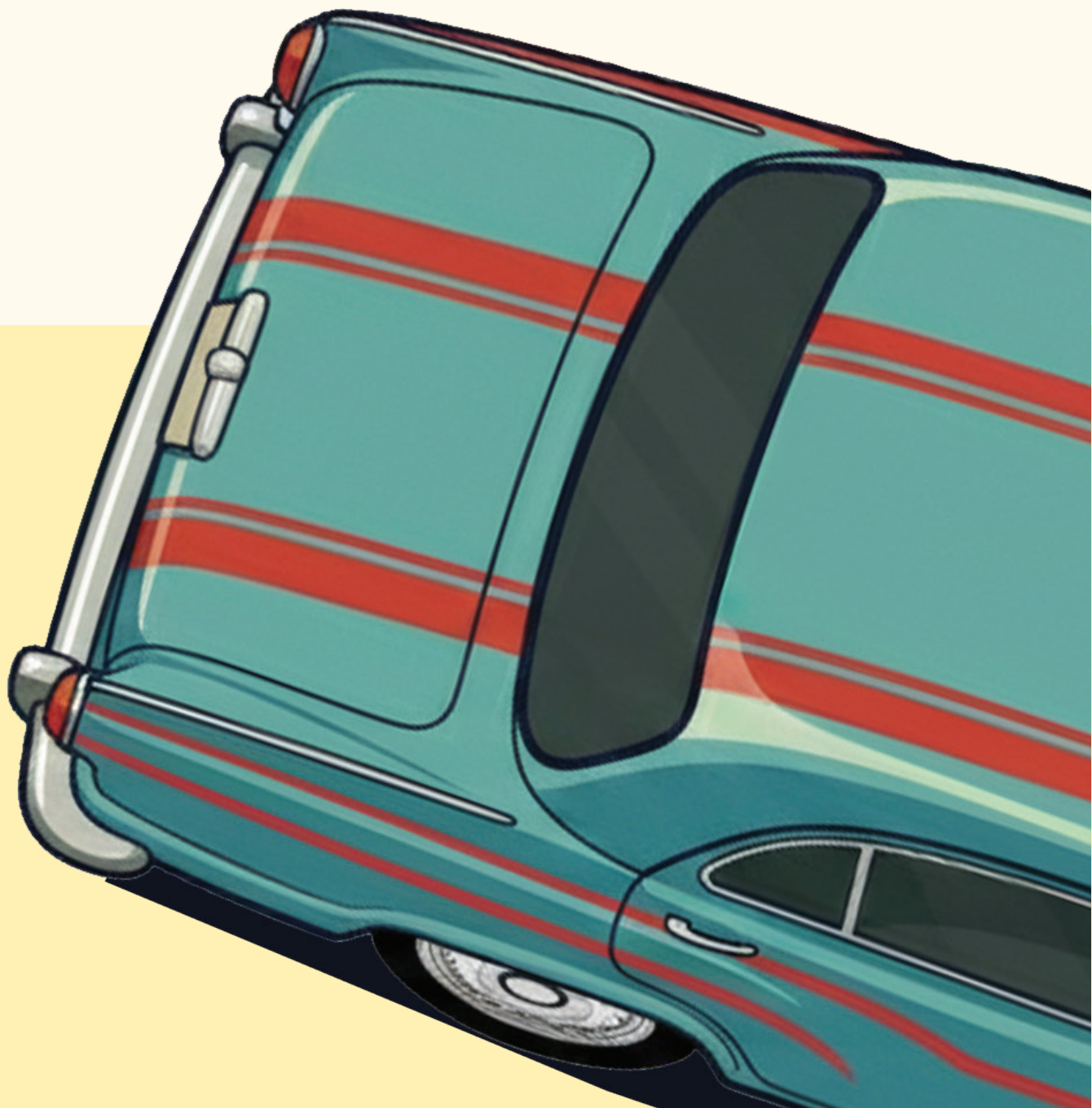
WHY THIS MATTERS?

Children and PwD are a vulnerable section of the population. Risks to any rights may have long and unwarranted consequences.



If adults deserve control over their data, children deserve even stronger protection.

WHEN THE LAW DOES NOT APPLY



WHEN YOUR DATA FALLS OUTSIDE THE LAW

The DPDP Act is designed to protect your personal data but it does not apply in every situation. There are certain cases where personal data falls outside the scope of the law. Understanding these limits help you make safer and more informed choices online.

THE DPDP ACT MAY NOT APPLY WHEN:



You voluntarily share your personal data openly, the law may not protect it.

For example

- * Your phone number, email ID, or address shared on a public social media profile.
- * Photos or videos you post on public social media platforms.
- * Personal details shared openly in public forums or comment sections.



What this means?

Before sharing personal information publicly, pause and consider who might access it and how it could be used later.



When in specific cases, personal data is made public because another person or authority is legally required to do the same.

For example

- * Names in voter lists published for the election.
- * Details of entity directors available on government portals.
- * Court judgments mentioning the names of parties.



What this means?

Not all public data is shared by choice, some disclosures exist to ensure transparency, accountability, or public interest.



When personal data is used strictly for personal or domestic activities, with no commercial or organisational involvement.

For example

- * Saving family or friends' contacts on your personal phone.
- * Sharing photos in a private family WhatsApp group.
- * Maintaining a personal diary or address book.



What this means?

Everyday personal use of data within private spaces is not regulated under the law.



If you make your data public, or the law makes it public, the DPDP Act may not apply. So always, think before you share!

THE DATA PROTECTION BOARD (DPB)



WHY AND WHEN TO APPROACH THE DPB?

The Data Protection Board (DPB) is a authority established under the DPDP Act, to enforce your rights under the framework.

A citizen may approach the Data Protection Board (DPB), or when an organisation does not address their data-related requests or complaints under the DPDP Act and when a complaint made by a Data Principal in respect of personal data breach or a breach by DF of obligations or a complaint made by DP in respect of breach by consent manager.

The DPB examines such complaints and takes action to ensure compliance with the law, thereby protecting the digital rights of citizens.

The Government has also issued a Notification establishing the DPB as the statutory enforcement body under the DPDP Act, with its head office located in the National Capital Region. The DPB is designed to function as a digital-first authority regulating processing of personal data and is empowered to receive breach notifications, conduct inquiries, issue directions, accept voluntary undertakings and impose monetary penalties for non-compliance. A further Notification confirms that the DPB will comprise four members at inception. Appointments to these positions are expected to follow the statutory selection process laid out under the DPDP Rules.



HOW A CITIZEN SHOULD PROCEED? (STEP-BY-STEP ROADMAP)

Here is a practical roadmap that explains how a citizen can proceed from checking a entity's privacy notice to approaching the Data Protection Board, if required.

STEP 1

Check the entity's notice

Every entity (Data Fiduciary) that uses your data is legally required to provide you with a Privacy Notice. This notice must contain a specific link or contact details that tell you how to exercise your rights and, most importantly, how to make a complaint to the Board if something goes wrong.

STEP 2

Use the internal grievance system

Exhaust internal grievance system of an entity. if complaint not resolved within 90 days, then you may approach DPB.

The business contact information of the Data Protection Officer, if applicable, or a person who is able to answer on behalf of the Data Fiduciary the questions of the Data Principal about the processing of her personal data. [Rule 9, DPDP Rules 2025]

STEP 3

Filing the digital complaint

The DPB follows its own procedures to examine cases and arrive at conclusions or decisions. It may also take suo motu cognisance of matters.

STEP 4

The Board's inquiry

Once you file, the Board will determine if there are sufficient grounds to investigate.

- * Examine the complaint
- * Seek explanations from the organisation
- * Call for information or documents if required

Timeline

The Board aims to finish its inquiry within 6 months, though it can be extended by an additional 3 months, if required for a valid reason.

STEP 5

The Final Order and Penalties

If the Board finds a violation, it may:

- * Direct the organisation to correct or delete your data
- * Order remedial measures
- * Impose penalties on the organisation
- * Fines: These can range from ₹50 crore for general violations up to ₹250 crore for failing to protect data with proper security.
- * **False Complaints:** Be careful, if the Board finds your complaint is false or frivolous, it can issue a warning or make you pay the costs of the proceeding.

STEP 6

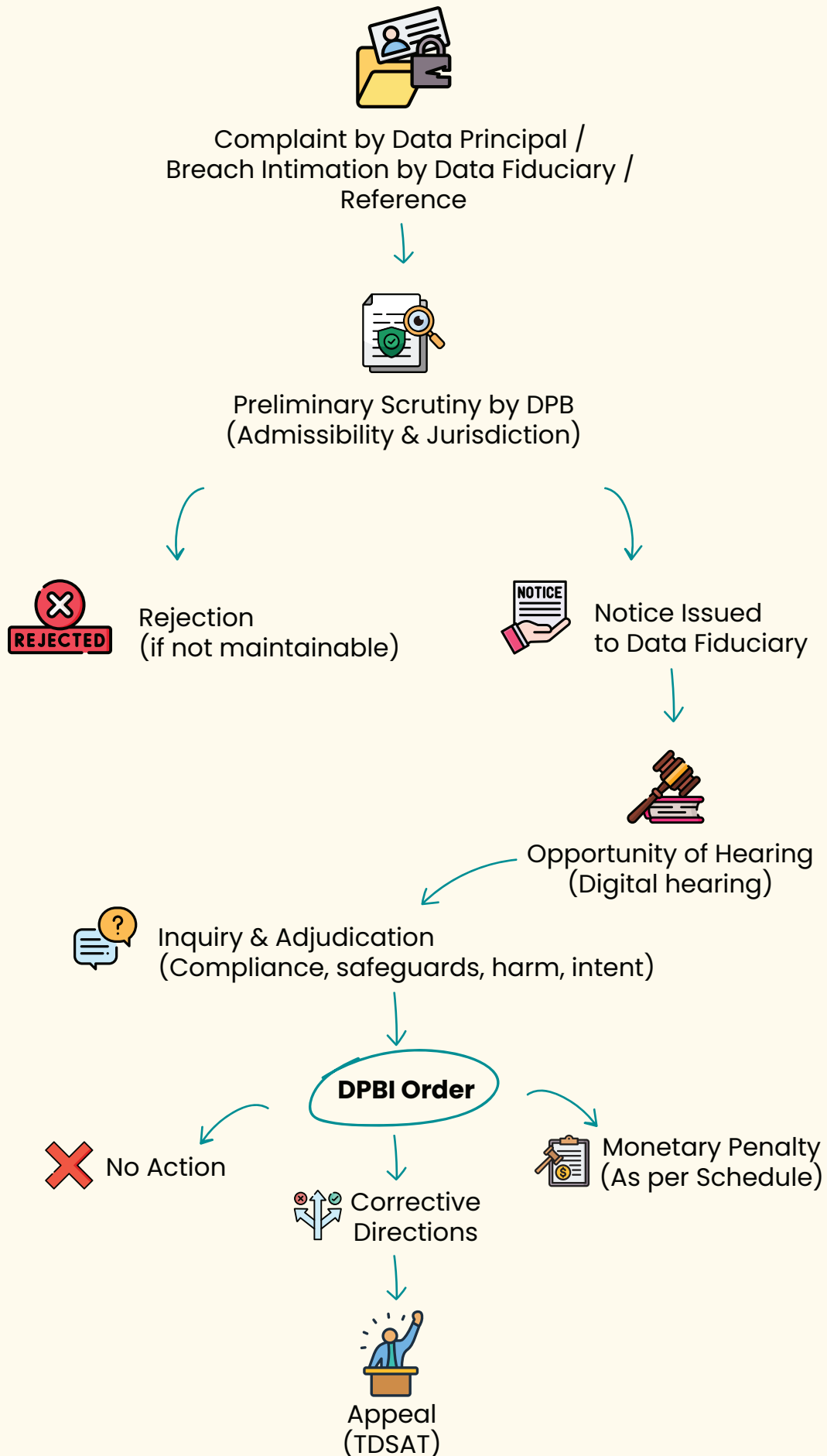
Appeal to TDSAT

If you are not satisfied with the decision of the Data Protection Board, you have the right to challenge it.

Appeals against decisions of the Data Protection Board lie before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).

- * **Timeline:** You must file the appeal within 60 days of receiving the Board's order.

LET'S BREAK IT DOWN FOR YOU!



PRIVACY DO'S AND DON'TS

Privacy is not only about laws and policies, it is shaped by daily choices and habits. Whether you are an individual citizen or an organisation, following these simple practices can significantly reduce risk and build trust.

DO'S

- ✓ Take a moment to understand why your data is being collected and how it will be used. Even a quick scan can help you spot unnecessary or risky data requests.
- ✓ Review app permissions regularly. Grant access only to what is essential for the service to function. Location, contacts, camera, and microphone access should never be given casually.
- ✓ If something feels wrong, unexpected messages, suspicious calls, or unauthorised use of your data, report it. Timely reporting helps prevent further harm.
- ✓ Consent is a choice, not a reflex. Use it carefully and withdraw it when it no longer serves a purpose.

FOR INDIVIDUALS/CITIZENS

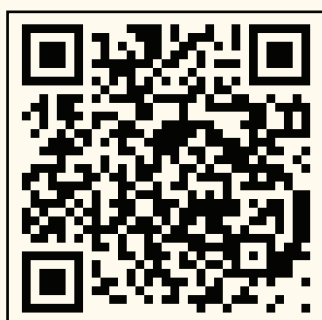
DON'TS

- ✗ Don't share sensitive details such as address, date of birth, identity numbers, or financial information unless absolutely necessary.
- ✗ "Agree" buttons may seem routine, but skipping consent screens can mean agreeing to data uses you did not intend.
- ✗ Links, pop-ups, and "free offers" can hide data collection traps. Pause, verify, and proceed with caution.
- ✗ Don't ignore updates and privacy setting changes. App updates often reset permissions or introduce new data practices that need your review.

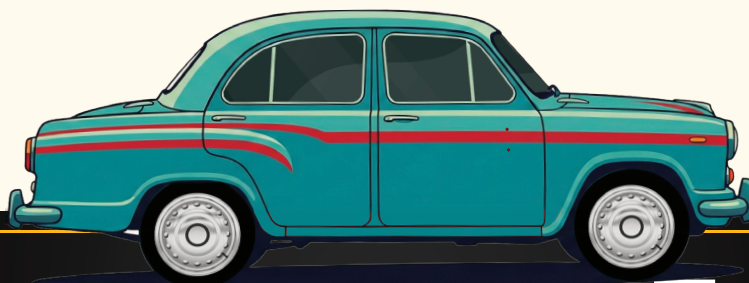
SUPPORTED BY



SCAN TO VISIT
DATA PRIVACY AWARENESS DRIVE



www.dsci.in/data-privacy-day-2026/





ABOUT DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, set up by Nasscom, committed to making cyberspace safe, secure, and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, Telecom and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.



Follow us on social media channels for more **Data Privacy Day 2026** awareness content!

Write to us: dpd@dsci.in | www.dsci.in

[X DSCI_Connect](#)

[f dsci.connect](#)

[@ dsci.connect](#)

[dscivideo](#)

[data-security-council-of-india](#)