Your Data, Your Rights:

Understanding India's Digital Personal Data Protection Act, 2023

By: Aayush Jain

Agenda – Part 1

01 Citizen First Approach

02 Global Context of Privacy

03 Data Breaches Happening Around the World

04 Key Definitions & Roles

05 Scope & Applicability

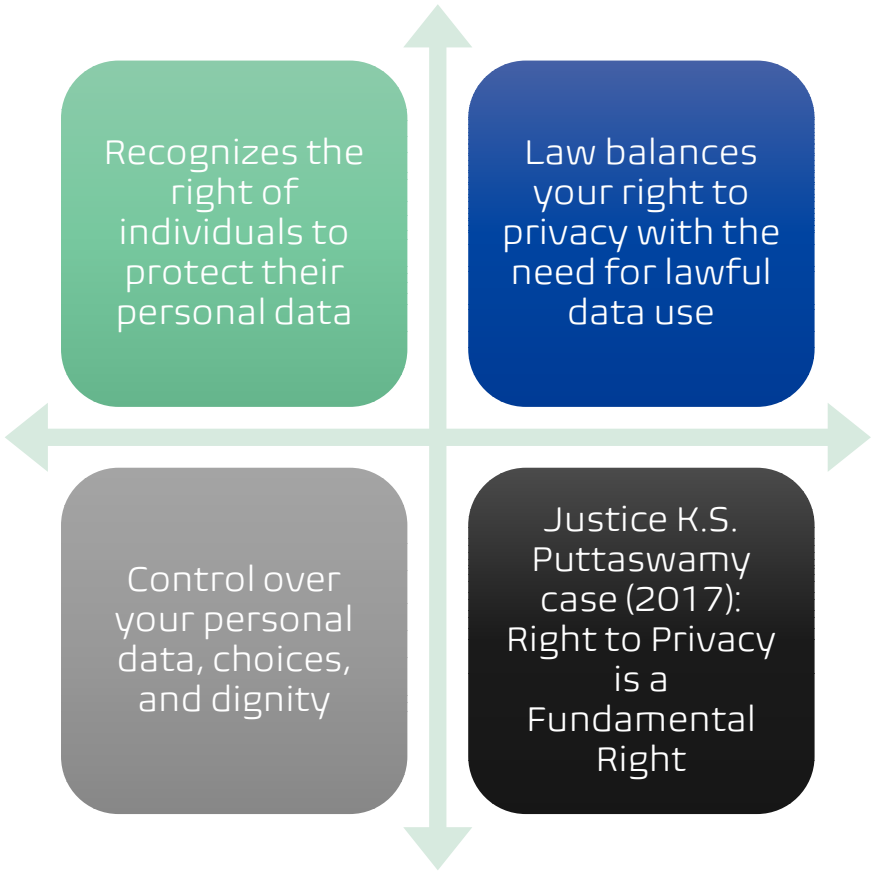
06 Grounds for Processing of Personal Data

07 Notice and Consent Mechanism

08 Rights and Duties of Data Principals

Your life is digital. This Act makes sure it's also private

Citizen First Approach



Right to Equality

Right to Freedom

Right against Exploitation



How many of you have clicked ‘I Agree’ without reading the privacy notice?

How many have ever shared your Aadhaar/PAN copy on WhatsApp or email without thinking twice?

Feeling Hungry lets order some food ?

Global Context of Privacy



- Worldwide Trend
  - Over 130 countries have enacted privacy legislation
  - India is coming now – being the latest major economies to implement
- GDPR & Other Law
  - GDPR (2018) setting high standard
  - DPDP Act shares similar principles but covers only digital personal data
- Why it Matters
  - Data breaches and scandals
  - Aiming to protect citizens while facilitating cross-border data flows and trade.

Data Breaches Happening Around the World



- ICMR COVID-19 Data Breach, India (2023)
  - A major cybersecurity incident at the Indian Council of Medical Research (ICMR) where an exposure happened.
    - 815 million individuals. Data included names, Aadhaar numbers, passport info, phone numbers, addresses, and COVID test results

No Penalty Imposed



- Justdial Data Breach, India (2019)
  - Personal information of users was exposed because of an unprotected API / old insecure endpoints.
    - Over 100 million users. Data: names, mobile numbers, email IDs, occupations, addresses etc

Data Breaches Happening Around the World

- BigBasket Data Breach, India (2020)
  - Grocery delivery/online retailer's database was breached; data put up for sale.
    - 20 million users. Data: email IDs, password hashes, PINs, phone numbers, addresses, DOB, location, IP addresses

No Penalty Imposed

- Air India / SITA Passenger Data Breach
  - Systems of SITA (an airline data service provider) were compromised; many airline customers' data exposed.
    - Passengers from Air India, Singapore Airlines, Lufthansa etc. Personal data of those who booked flights from 2011-2021

Data Breaches Happening Around the World

Organization	What went wrong	Penalty
Meta	Transferring personal data of European users to the U.S. without adequate data protection safeguards (standard contractual clauses etc.) violated GDPR	€1.2 billion (~US$1.3 billion) by the Irish Data Protection Commission in 2023. In INR = 1.07 lakh crore
Google (France)	Failed to provide clear, transparent user info about how it uses personal data for advertising; did not get valid consent	€50 million fine (2019) In INR = ₹445 crore
TikTok / Ireland	Transferring EU user data to China without adequate safeguards; also insufficient clarity in policy about those transfers	€530 million fine In INR = ₹4,717 crore

Key Definitions & Roles

Data	Information or facts that can be understood by people or computers. It could be anything from words to numbers.
Personal Data	Information about a person that can help us figure out who they are. It could be things like their name, age, or where they live.
Digital Personal Data	Personal data exists in electronic/digital form (e.g., stored on a computer, cloud, app, or converted from paper to digital), it becomes digital personal data.
Data Principal/Data Subjects	The individual to whom the personal data relates

Key Definitions & Roles

Data Fiduciary – The CEO	An entity (individual, company, firm, government agency, etc.) that determines the purpose and means of processing personal data
Data Processor – The Employee	An entity that processes personal data on behalf of a Data Fiduciary
Consent Manager – The HR Manager	A service provider acting as a centralized agent for managing consent
Significant Data Fiduciary (SDF) – The Conglomerate	A Data Fiduciary classified by the government as significant based on factors like volume and sensitivity of data processed, risk to individuals' rights and impact on national interests
Data Protection Board of India (DPB) – The Compliance Officer	The regulatory authority established by the Act to oversee compliance, adjudicate disputes and impose penalties.

Examples of Personal Data

Direct identifiers

- Full Name
- Date of Birth / Age
- Gender
- Photograph, Video, or Audio recordings
- Contact details: Phone number, Email address, Residential address

Govt Identifiers

- Aadhaar number
- PAN number
- Passport number
- Driving license number
- Voter ID
- Ration card number

Financial Data

- Bank account details
- Credit/debit card numbers
- Loan account numbers
- Investment details
- Insurance policy numbers

Online & Digital Identifiers

- IP address
- Device IDs (IMEI number, MAC address)
- Cookies or tracking IDs
- Social media handles or login IDs
- Location data (GPS coordinates, check-ins)

Examples of Personal Data

Employment & Education Data

- Employee ID
- Salary or payroll information
- Employment history
- Qualifications, marksheets, transcripts
- Professional licenses

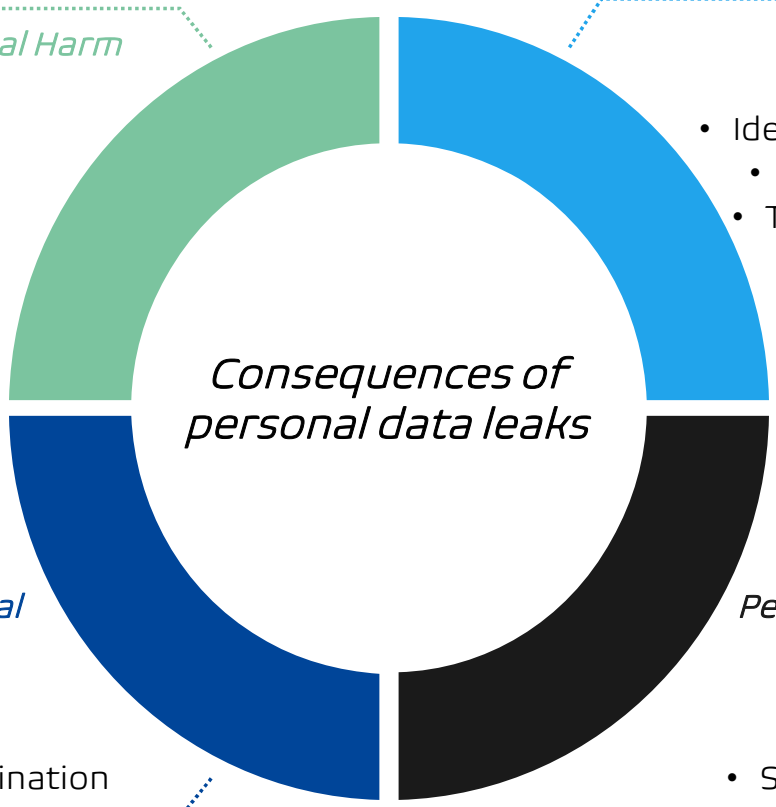
Sensitive / Special Category Data

- Health data (medical records, prescriptions, genetic information)
- Biometric data (fingerprints, facial recognition, iris scans, voice patterns)
- Disability information
- Children's data

Other Contextual Personal Data

- CCTV footage where individuals can be identified
- Customer feedback linked to identity
- KYC documents (scanned ID proofs)
- Travel history (flight, train, hotel bookings with name/ID)

If personal data is leaked – what can go wrong?



Emotional & Psychological Harm

- Emotional distress
- Anxiety
- Loss of trust
- Long recovery from breach trauma

Financial & Identity Risks

- Identity theft & financial loss
- Account takeover & fraud
- Targeted phishing & scams

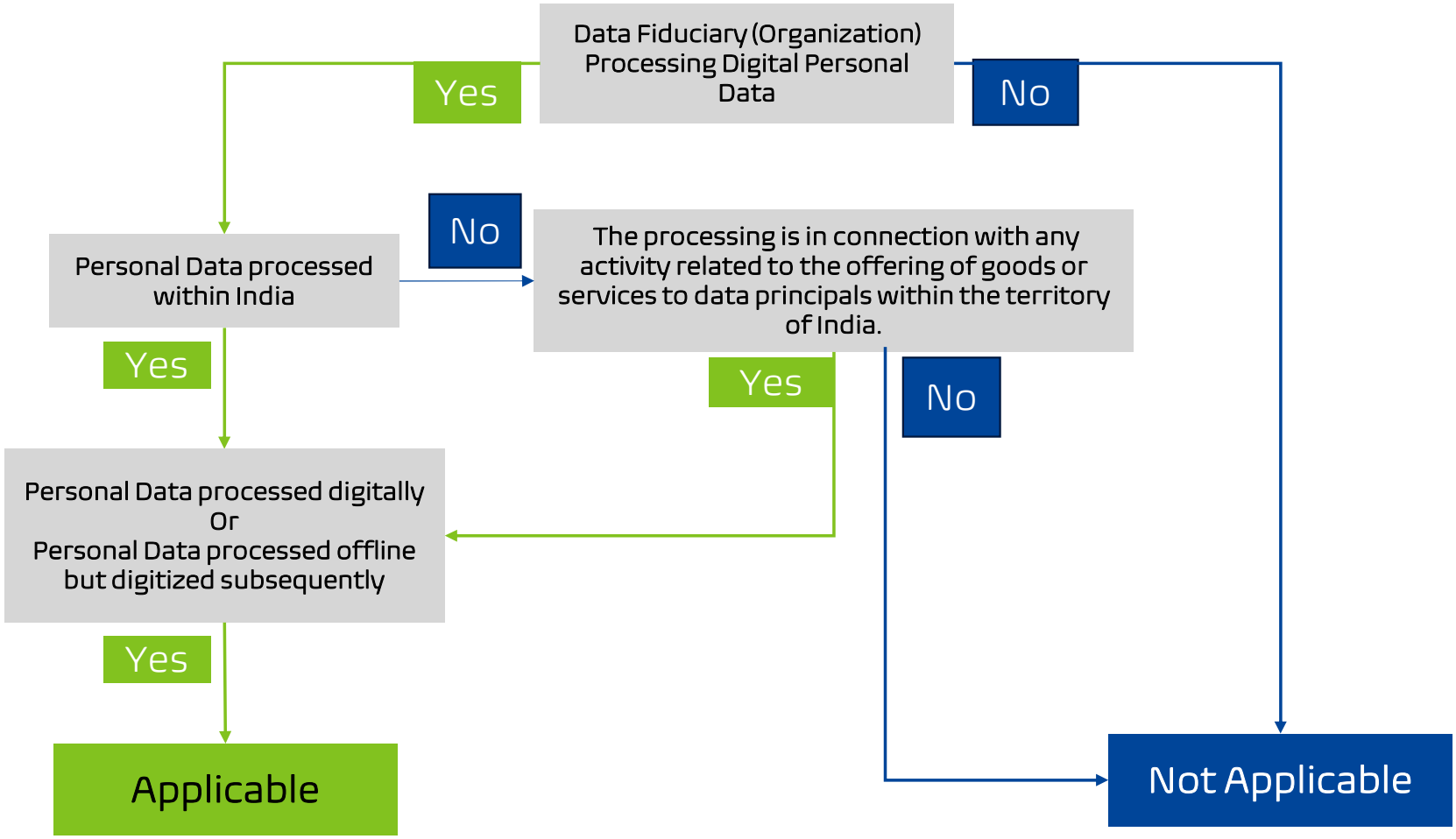
Reputation & Professional Impact

- Reputation damage
- Employment & discrimination

Personal Safety & Sensitive Exposure

- Blackmail / extortion
- Stalking & physical danger
- Medical & insurance harm

Scope & Applicability

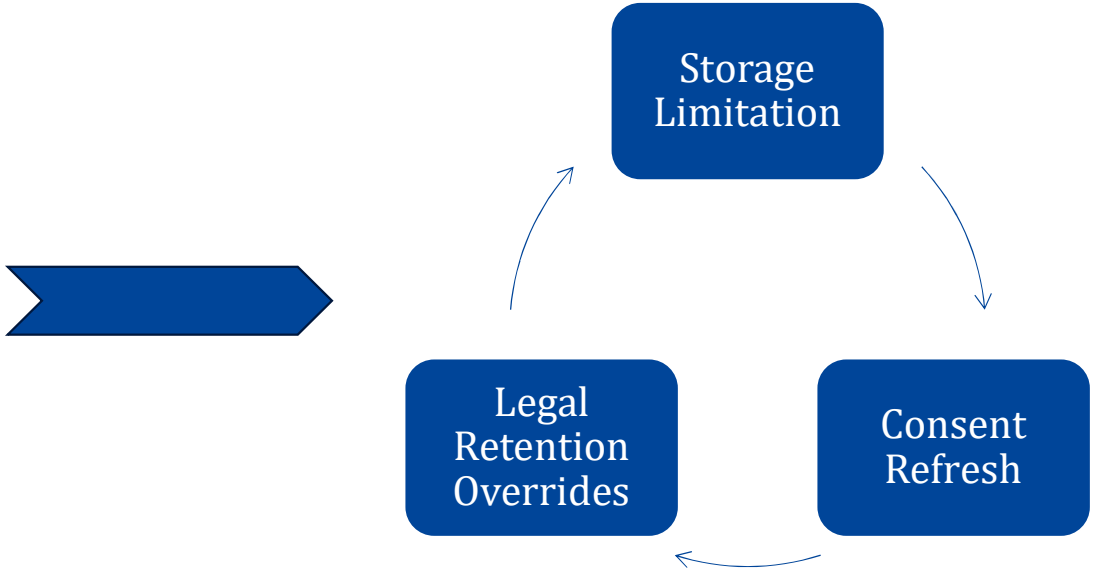


Applicability – Old Data ????

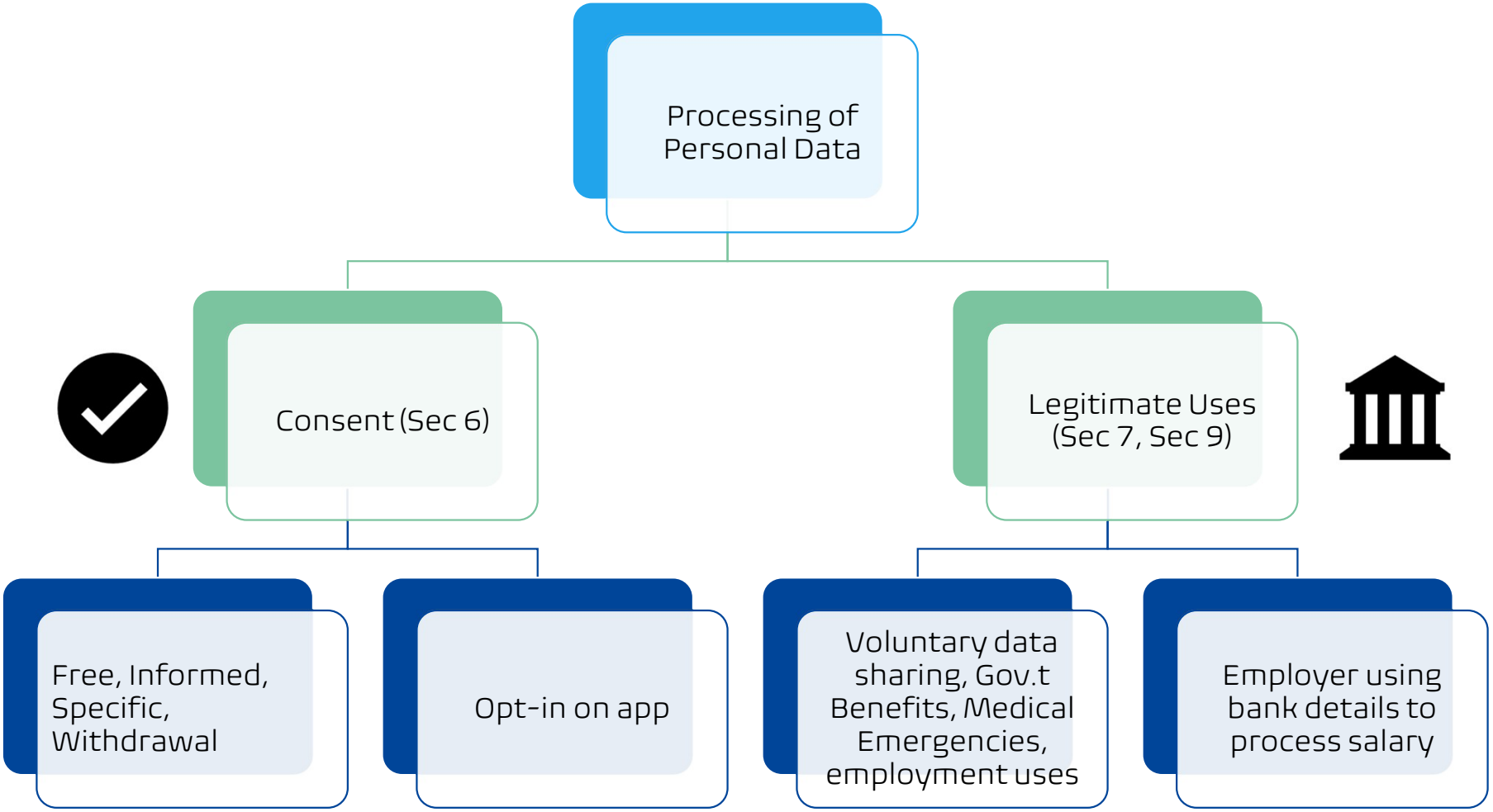
Does the Act apply to old data?

Yes

All personal data in digital form that is stored or processed after the Act comes into force, even if it was collected years ago



Grounds for Processing Personal Data



Grounds for Processing Personal Data

New members must complete this form on joining. Existing members will be asked to confirm their consent at regular intervals.

Name * Name * Name *

Title | First Name | Surname

Please indicate your agreement to the following statements *

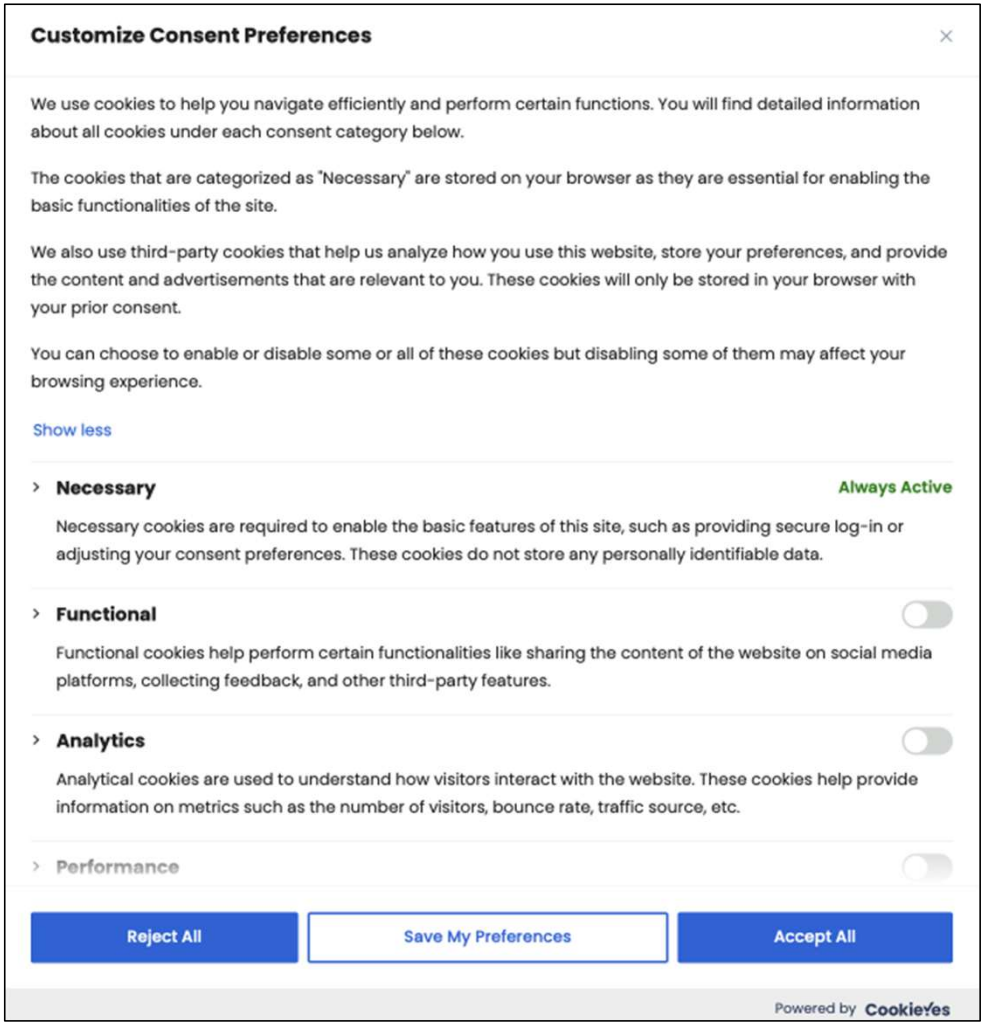
- ☐ I have read and accepted the GDPR Policy
- ☐ I consent to the Club contacting me by Phone (includes by SMS)
- ☐ I consent to the Club contacting me by E-mail
- ☐ I consent to the Club contacting me by Post
- ☐ I consent to the collection of my ethnicity data
- ☐ I consent to the collection of my disability data
- ☐ I consent to the Club passing my details to GBA and BE for the purposes of affiliation to them
- ☐ The Club may publish my Name, Phone Number and E-mail address in the Club Directory (available only to club members)

Signature *

By typing your name you agree to our T&Cs

Submit

If you do not wish to submit the form online, you may also download a copy from the links below and either send the completed form by e-mail to cheltwhaddonbc@gmail.com . You may also print out the form and send it to the Club Secretary at the club address.



Grounds for Processing Personal Data – **Children's Data**

YouTube / Disney = Personalized Ads for Kids

- Minors under 18, verifiable parental consent
- Data Fiduciaries must not use children's data in harmful ways like:
  - No tracking
  - No targeted advertising
  - No behavioural profiling

Notice & Consent Mechanism

Mobile wallet app asks for permission to access your contacts

1. Notice before consent

-> Personal data will be collected

-> Purpose of processing

-> Person's rights

-> How to file compliant to DPB

2. Consent Requirement

-> Free (Voluntary)

-> Specific to purpose

-> Informed

-> unambiguous

3. Consent Withdrawal & Consequences

-> Simple as a click or an email

-> Data Fiduciary must stop processing their data for that purpose

4. Obligation to confirm consent

-> Data Fiduciary should provide a means to confirm that consent was given

-> Sending a confirmation email or dashboard notification to confirm what consented to

5. Penalties for invalid consent

-> Data Fiduciary fails to adhere to these notice

-> Consent obtained could be deemed invalid

-> DPB imposes penalty

Rights of Data Principals

01

Right to Information about Personal Data

02

Right to Correction

03

Right to Erasure

04

Right to Grievance Redressal

05

Right to Nominate

Duties of Data Principals

01

Not to impersonate another person

02

Not to furnish false particulars, or suppress any material information

03

Avoid Unnecessary complaints

04

Comply with applicable laws

05

Penalty for Breach of Duties


Right to Information
Rights in Action
Social Networking Site
Data Principal
Right to Correction
Escalation to DPB
Grievance Redressal
Right to Erasure

Agenda – Part 2

01 Obligations of Data Fiduciaries and Processors

02 Industry Impact

03 Cross-border Transfer of Personal Data

04 Exemptions under the Act

05 Personal Data Breach and Penalties

06 Information Security Practices

07 Current Status of Implementation

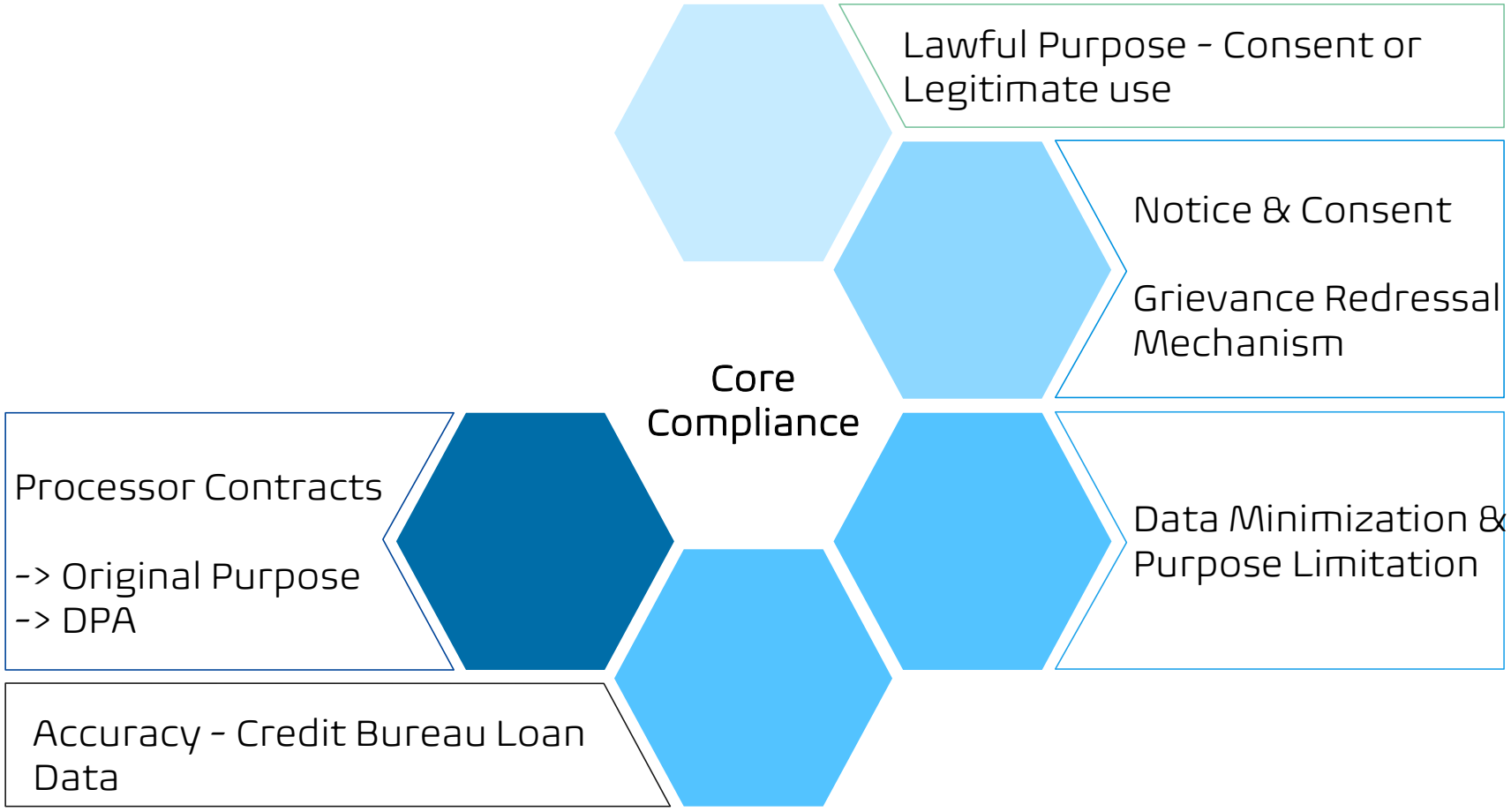
08 Misconception About DPDP

09 Comparison Between DPDP & GDPR

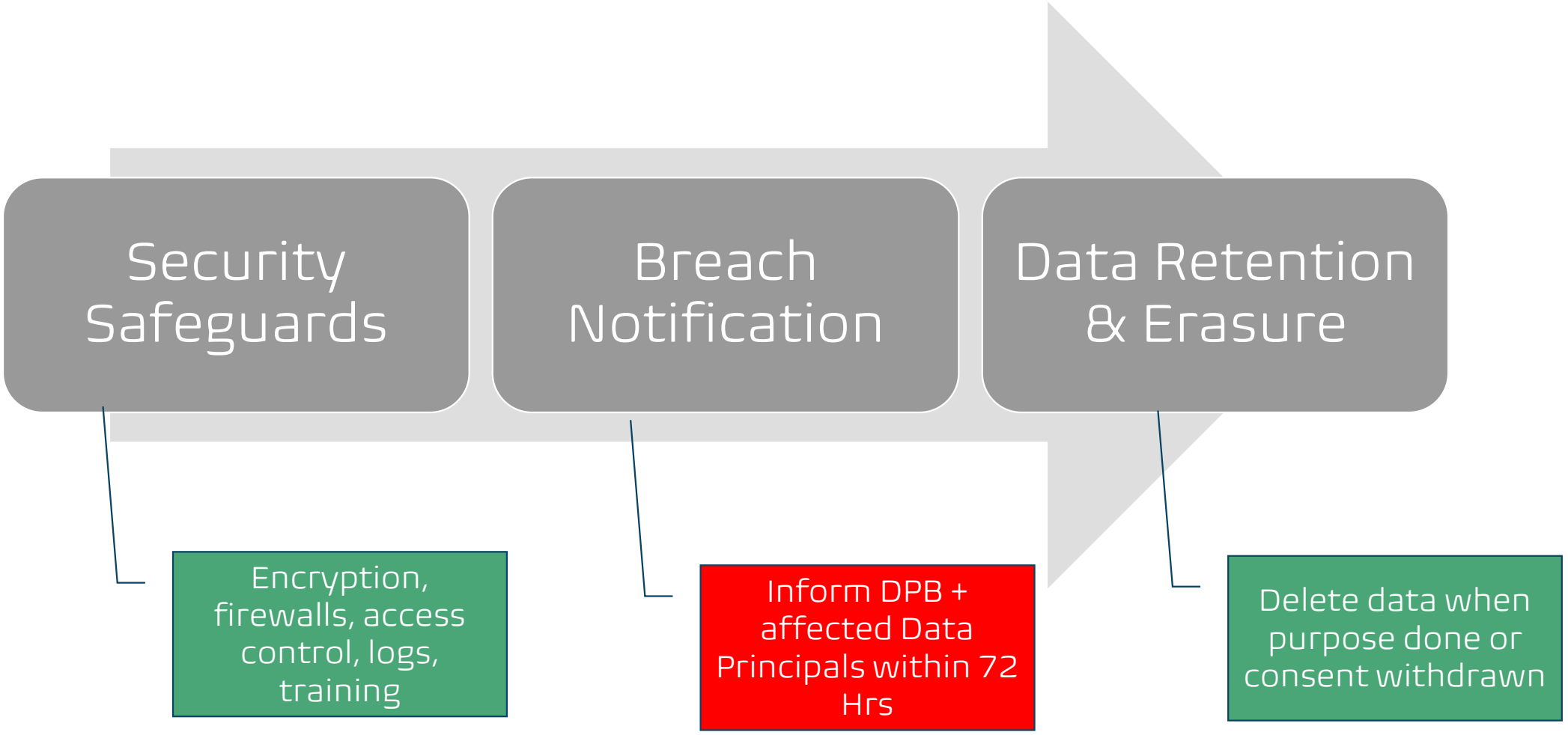
10 Interactive Quiz

11 Q&A Session

Obligations of Data Fiduciaries



Obligations of Data Fiduciaries



Obligations of Significant Data Fiduciaries

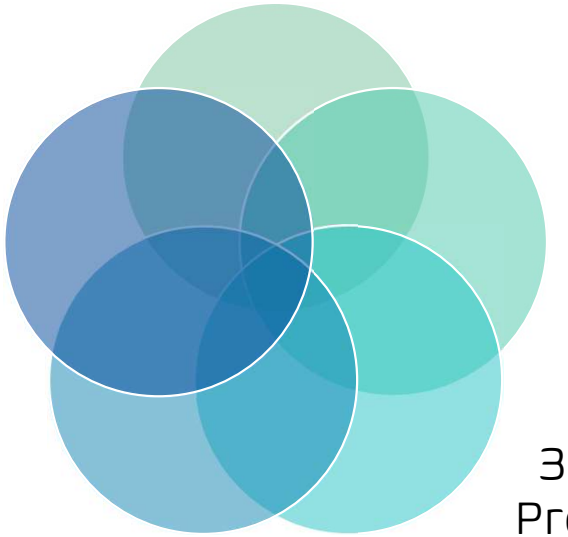
1. Appoint a Data Protection Officer (DPO)

2. Appoint an Independent Data Auditor

3. Conduct Data Protection Impact Assessments (DPIA)

4. Maintain Detailed Records of Processing

5. Enhanced Grievance Redressal Mechanism



Obligations of Data Processor

1. Process only as instructed by the Data Fiduciary

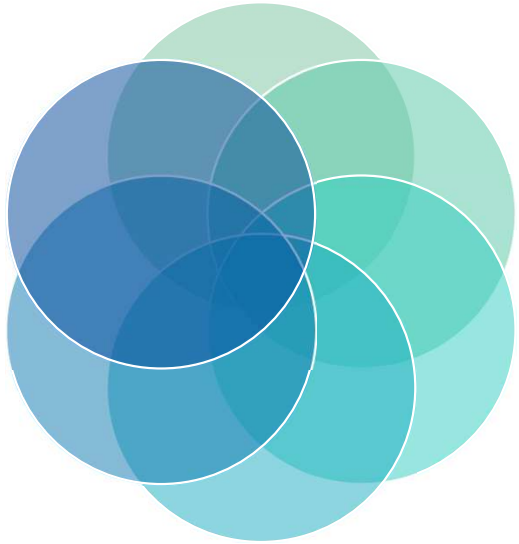
2. Confidentiality of all personal data handled

3. Implement security safeguards (technical & organizational)

4. Assist the Fiduciary in meeting compliance (e.g., breach notifications)

5. Bound by contract, must follow terms set by the Fiduciary

6. Indirect liability – if negligent, can face consequences via contracts or DPB proceedings



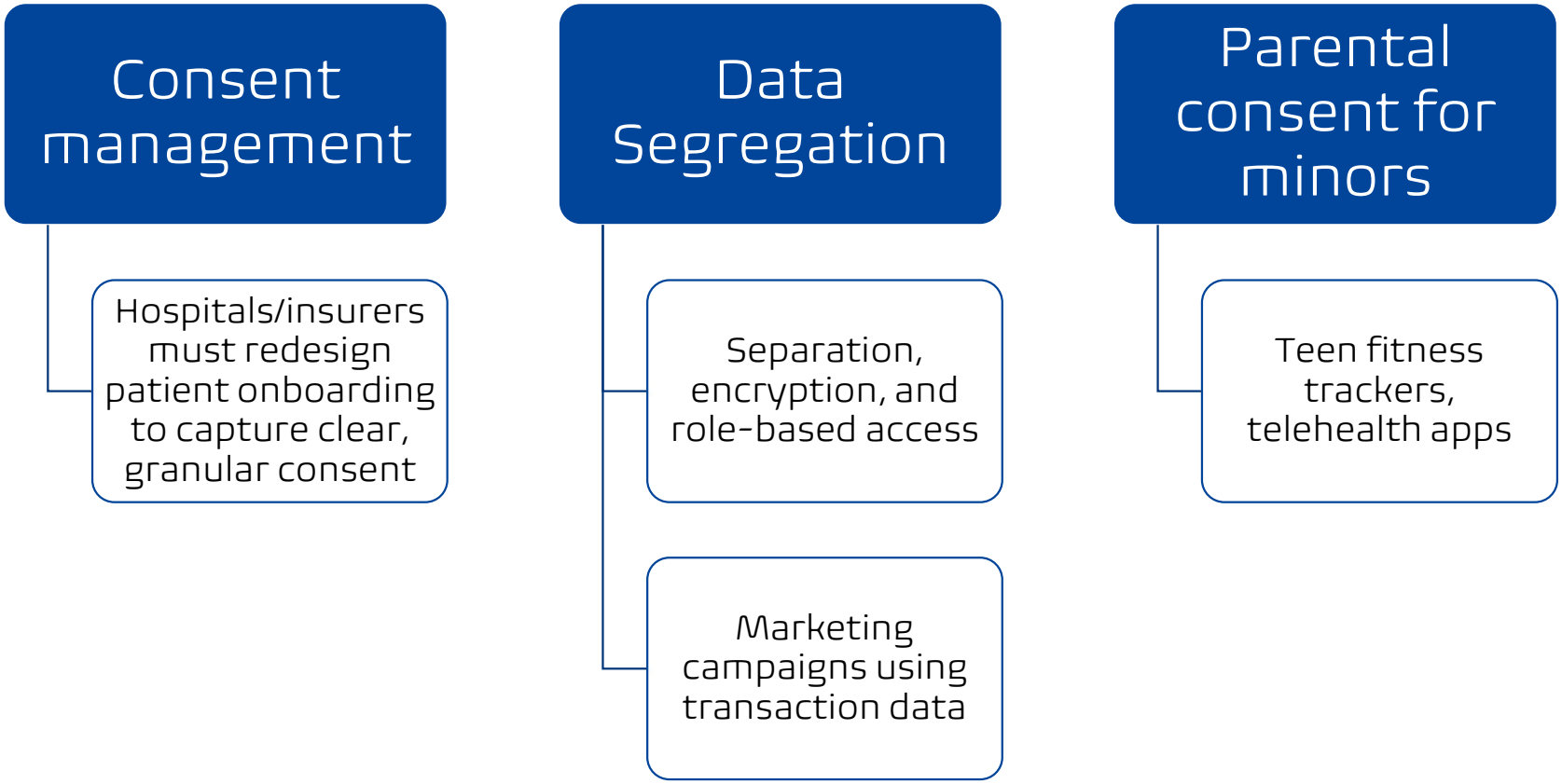
In Summary

Data Fiduciary & Data Processor must practice due diligence, transparency and accountability in all data operations

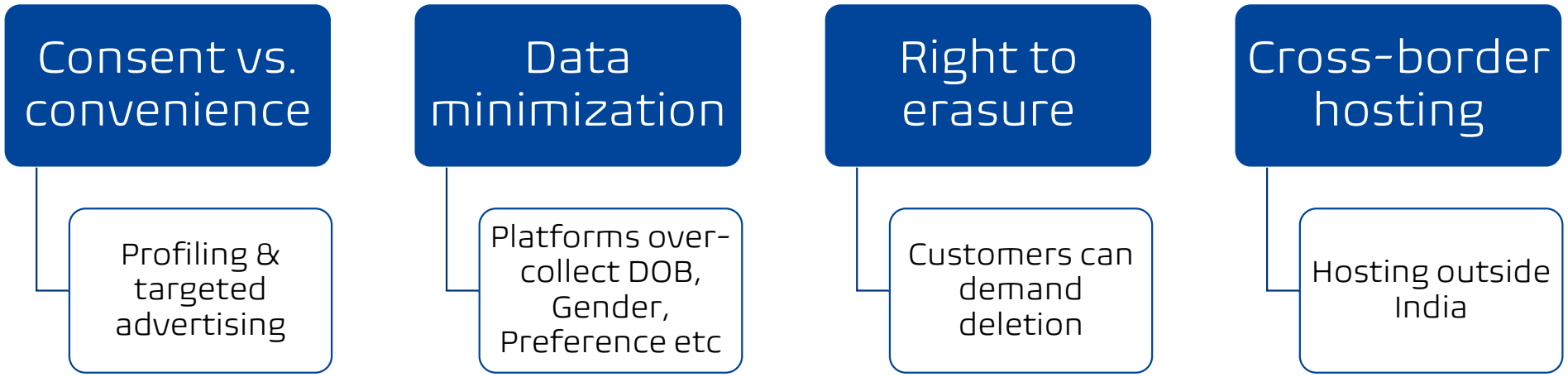
Industry Impact – Banking & Fintech

- **KYC Verification**
  - Aadhaar, PAN, Biometric Authentication
- **Pre-ticked boxes or bundled consent will no longer be valid**
  - Profiling for cross-selling (loans, insurance, wealth products)
  - Marketing campaigns using transaction data
- **Sharing data with fintech partners or third-party service providers**
  - Banks remain responsible for third party (Processor) mistakes
- **Data Retention Issues**
  - Customer data indefinitely for analytics, fraud detection, and future use
  - Erasure once purpose is over

Industry Impact – Healthcare



Industry Impact – E-Commerce



Industry Impact – EdTech

Age Verification

- Must verify if a user is a minor before processing

Parental consent

- EdTech apps must create reliable parental authentication

Ban on profiling children

- EdTechs using behavioral analytics for personalization

SDF compliance

- Need DPO, DPIAs, third-party audits.

Cross-Border Transfer of Personal Data

🟢 **Allowed by Default** – All countries unless restricted.

→ No Data Localization (Fintech storing data in Singapore or US → allowed, unless later blacklisted)

🟡 **Safeguards Needed** – Valid contracts with foreign processors / fiduciary, accountability of Indian fiduciary.

🔴 **Restricted Transfers** – If Govt. blacklists a country.

Accountability: Indian Fiduciary remains liable for breaches abroad, must notify DPB + affected users.

Exemptions under DPDP Act

When the Law Doesn't Apply

1. Legal Proceedings - Court summons requiring address disclosure

2. Law Enforcement - Police using call records in a fraud probe

3. Non-Indian Data Principals - Indian IT company processing EU client data.

4. Mergers & Corporate Restructuring - Sharing employee/customer data during due diligence

Exemptions under DPDP Act

When the Law Doesn't Apply

5. Credit Scoring - Banks/credit bureaus can process for financial defaults.

6. Public Interest Exemptions - Sovereignty, national security, friendly foreign relations, public order.

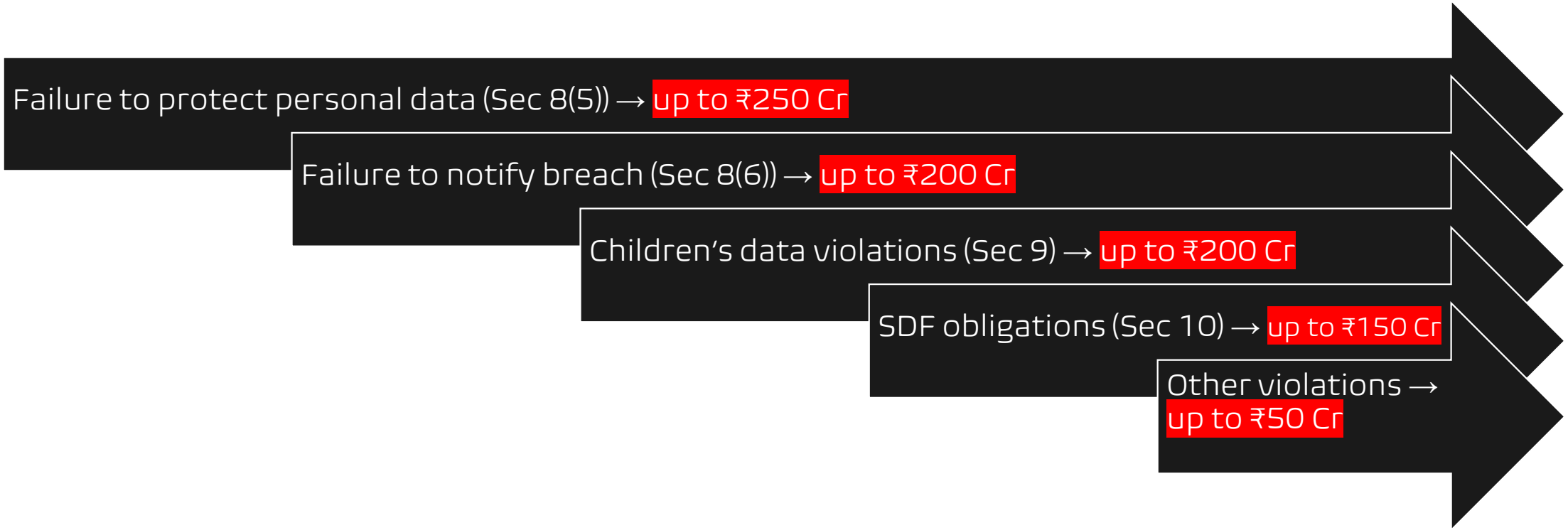
7. Small Entities & Startups – Few Section & Rules

8. Research, Archival, Statistical Uses

Personal Data Breach and Penalties

Data Breaches = Big Penalties

False complaints by individuals → up to ₹10K



Scenario	Breach Type	Possible Penalty
Fintech suffers hack due to weak security controls	Failure to implement reasonable safeguards	💣 Up to ₹250 Cr
Company delays breach notification to users	Breach of notification duty	💣 Up to ₹200 Cr
An app tracks children without parental consent	Breach of obligations for children's data	💣 Up to ₹200 Cr
Social media giant ignores SDF audit requirements	Breach of SDF obligations	💣 Up to ₹150 Cr
Startup ignores user's request to delete profile	General non-compliance	💣 Up to ₹50 Cr
Citizen files false complaint	Breach of duties	⚠️ ₹10K fine

How Security Practices Enable Privacy Compliance

ISO 27001 (ISMS)

&

ISO 27701 (PIMS)

DPDP Act Privacy Obligation	Information Security Practice
Lawful Processing & Consent	• Consent management systems • Audit trails • Privacy dashboards for withdrawal.
Data Minimization & Purpose Limitation	• Role-based access • System design to collect only necessary fields • Periodic data reviews.
Data Accuracy	• Validation checks • User self-service portals for updates • Data quality audits
Children's Data Protection	• Age verification controls • Parental consent workflows • Disable profiling/targeted ads for minors
Security Safeguards	• Encryption (data at rest & in transit) • MFA • Firewalls • EDR • Employee awareness training

How Security Practices Enable Privacy Compliance

DPDP Act Privacy Obligation	Information Security Practice
Breach Notification	• Incident detection & response plan • SIEM monitoring • Breach reporting workflows
Data Retention & Erasure	• Automated deletion policies • Data retention schedules • Secure wiping processes
Third-Party & Cross-Border	• Vendor due diligence • Data Processing Agreements • Secure data transfer contracts
Transparency & Accountability	• Published privacy notices • Grievance redressal systems • Compliance dashboards
Significant Data Fiduciary Obligations	• Appointment of DPO • DPIAs • Periodic independent audits

Current Status of Implementation

Enactment & Status

- **Passed**: August 11, 2023 (Presidential assent).
- **Law in Force**: Act notified, but provisions not yet operational.
- **Phased Rollout Planned**: Different sections will be enforced at different times.
- **Pending**: Data Protection Board (DPB) not yet constituted → enforcement on hold.

Current Status of Implementation

Draft Rules 2024/25

- **Draft DPDP Rules 2024** released in Jan 2025 for public consultation.
- Cover procedural details:
  - Consent notices
  - Breach reporting format (72 hrs)
  - Consent Manager registration
  - SDF compliance requirements
- DPDP rules followed by a comprehensive set of FAQ's to be released by 28 September

Current Status of Implementation

Companies preparing via:



PRIVACY POLICY UPDATES



GAP ASSESSMENTS



BASIC POLICIES AND PROCEDURES



PRIVACY RISK ASSESSMENT

Misconceptions About DPDP

- This law stops all data collection → False
- Only big companies need to comply → False
- It replaces cybersecurity laws → False
- Consent is always required → False
- Data can be stored forever if consent is given once → False
- Individuals can demand anything under DPDP → False
- Penalties apply only when there's a breach → False
- Cross-border transfer is always free if user agrees → False

Comparison Between DPDP & GDPR

Aspect	DPDP Act, 2023 (India)	GDPR (EU)
Scope	Applies to digital personal data of individuals in India; extraterritorial if goods/services offered to Indians.	Applies to all personal data (digital + offline) of individuals in EU; extraterritorial worldwide.
Legal Bases	Only Consent + limited legitimate uses (e.g., govt. benefits, employment, emergencies).	Multiple bases: consent, contract, legal obligation, vital interests, public task, legitimate interests.
Consent	Must be free, informed, specific, unambiguous, and revocable. Consent Managers allowed.	Must be explicit, informed, specific, unambiguous. Special rules for sensitive data.
Individual Rights	Access, correction, erasure, grievance redressal, withdraw consent, nomination of heir.	Access, rectification, erasure, portability, restriction, objection, no automated profiling without safeguards.
Penalties	Up to **₹250 Cr (€27M)** for major breaches.	Up to **€20M or 4% of global turnover**, whichever is higher.

Quiz Time

1. The DPDP Act, 2023 applies to which of the following scenarios?

A. Personal data collected in paper forms and never digitized.

B. Personal data collected online from individuals in India by a foreign company offering services in India.

C. An individual processing personal data for purely domestic purposes (like a personal contacts list).

D. Personal data made public by the individual themselves on a social media profile.

Correct Answer: B

Quiz Time

2. Who is considered the “Data Principal” under the Act?

A. The company that decides why and how personal data is processed.

B. Any entity that processes data on behalf of another entity.

C. The individual to whom the personal data relates.

D. A consent management service appointed by a user.

Correct Answer: C

Quiz Time

3. According to the DPDP Act, which statement about consent is FALSE?

A. Consent must be free, specific, informed and unambiguous for it to be valid.

B. A Data Principal can withdraw their consent at any time.

C. Once given, consent cannot be withdrawn by the Data Principal.

D. Processing of personal data can occur without consent if it falls under certain legitimate uses.

Correct Answer: C

Quiz Time

4. Which of the following is NOT listed as a "certain legitimate use" (i.e., an allowed processing without explicit consent)?

A. Processing necessary for a medical emergency involving the individual.

B. Processing of data for the performance of a contract with the individual, when the individual hasn't given consent.

C. Processing by the State for providing a subsidy or service the individual applied for.

D. Processing of personal data that an individual voluntarily provided for a specific purpose.

Correct Answer: B

Quiz Time

5. Which right do Data Principals not have under the DPDP Act, 2023?

A. The right to obtain a summary of their personal data being processed by a company.

B. The right to correction of inaccurate personal data.

C. The right to demand transfer of their personal data from one service provider to another (data portability).

D. The right to nominate a person to exercise their data rights in case of death or incapacity.

Correct Answer: C

Quiz Time

6. Which of these is NOT an obligation of Data Fiduciaries under the DPDP Act?

A. To implement reasonable security safeguards to prevent data breaches.

B. To erase personal data when the purpose is fulfilled and retention is not required by law.

C. To notify the Data Protection Board and users of any personal data breach.

D. To publicly disclose the source code of all algorithms used in personal data processing.

Correct Answer: D

Quiz Time

7. Under the Act, processing personal data of children (below 18) requires:

A. Consent of the child if above 13 years of age; below 13 no consent is needed.

B. Verifiable consent of the child's parent or legal guardian in all cases.

C. No special requirements; children's data is treated same as adults.

D. Only government agencies can process children's data without consent.

Correct Answer: B

Quiz Time

8. Which scenario would not be exempt from Data Principal rights and fiduciary obligations under the Act?

A. A police department processing data for investigation of a cybercrime.

B. A private hospital processing health data of a patient for treatment (with patient's consent).

C. An intelligence agency processing data in the interest of national security, after being exempted by central government notification.

D. A bank processing defaulters' personal data to trace assets during a loan recovery (under IBC proceedings).

Correct Answer: B

Quiz Time

9. The Act creates a category of 'sensitive personal data' with higher protection requirements than other personal data

A. True

B. False

Correct Answer: False

Quiz Time

10. A Data Principal is entitled to request erasure of their personal data, but the Data Fiduciary may refuse if the data needs to be retained for legal compliance.

A. True

B. False

Correct Answer: True

Quiz Time

11. If a company fails to implement proper security safeguards and a major data breach occurs, it can face a penalty of up to Rs. 250 crore under the DPDP Act.

A. True

B. False

Correct Answer: True

Q & A

Thank You

Aayush Jain



9940221905



Aayush@protaxology.com