

DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Compliances and Obligations



யாகாவா ராயினும் நாகாக்க காவாக்கால்
சோகாப்பர் சொல்லிழுக்குப் பட்டு

Guard your tongue; Unguarded words cause distress.



PRIVACY IS POWER.

*WHAT PEOPLE DON'T KNOW, THEY
CAN'T RUIN*



WHAT IS 'PRIVACY'

**FREEDOM TO
EXPRESS**

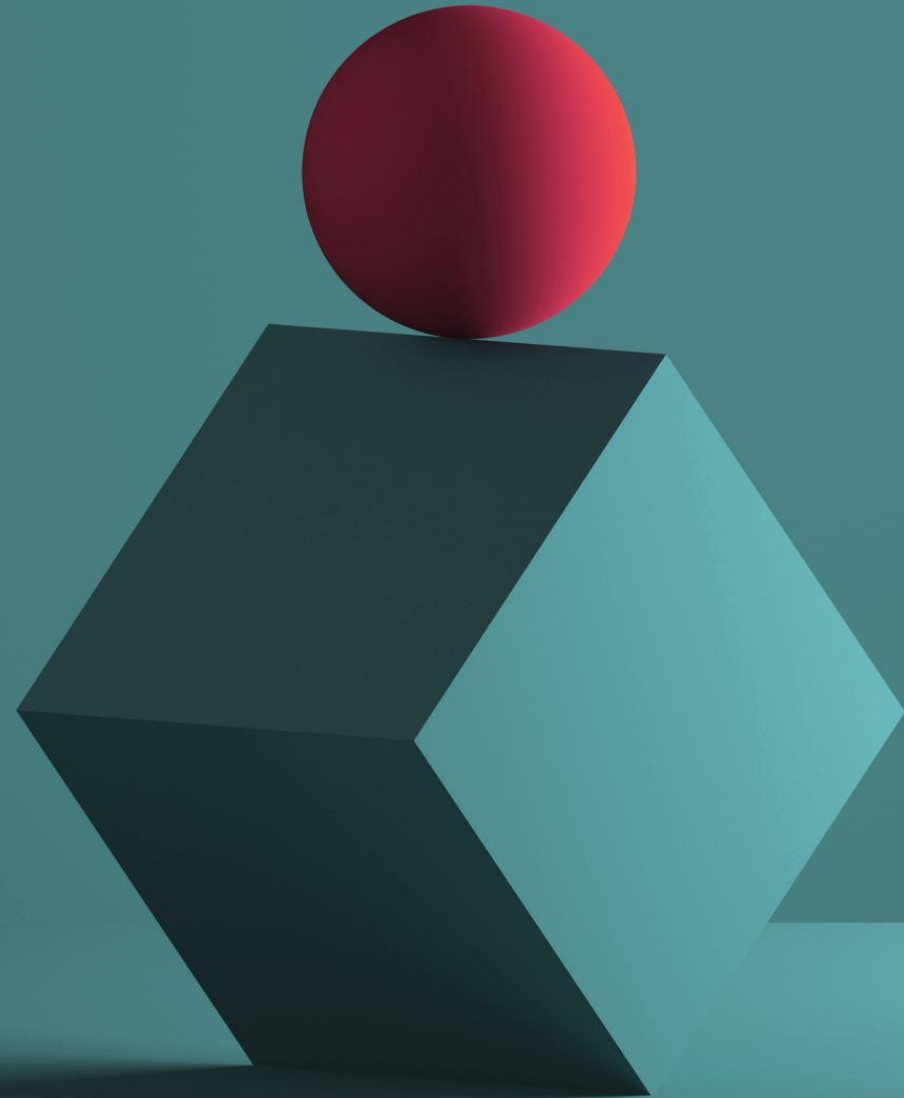
VS

RIGHT TO PRIVACY

**FREEDOM TO
EXPRESS**

WITH

RIGHT TO PRIVACY



DATA IN DIGITAL ECONOMY



Data is called the new oil



Data holds tremendous value



Data now powers industries



Like oil data can impact the environment, unless it is processed properly

INDIA AND DATA

- India is the largest connected democracy in the world
- 'Digital India' initiatives have caused digitization of the Indian economy.
- Unleashed innovation and entrepreneurship in the digital space.



Taxi Company
No vehicles



Valuable
retailer
No inventory



largest food delivery
provider
No restaurants



Largest accommodation
provider,
no real estate



Popular media
owner,
No content created

YOU ARE YOUR DATA

- Using mobile applications
 - Fitness Apps
 - Music Apps
 - News Apps
 - Social Media
- Transactions with banks, financial institutions
- As a student subscribe for an online course
- As a Parent you share your children data

IS YOUR DATA SAFE?

- Internet and technology is a force for good and connectivity, it is also a place where user harm and misuse can exist if these rules and laws are not prescribed.
- Increased incidents of data breaches
 - 2.29 bn records were exposed worldwide. India accounts for 20% of the total – II position
- Individual Level concerns / risk
- Organizational Level risks
- Societal and Government Level Concerns
- That is why laws and rulemaking for the internet has to be around the basic foundational principles

DIGITAL PERSONAL DATA PROTECTION ACT, 2023



The Making Of The Digital Personal Data Protection Act, 2023

| | |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| July 2017 | <ul style="list-style-type: none">MeitY constitutes an expert committee under the chairmanship of Justice BN Srikrishna |
| August 2017 | <ul style="list-style-type: none">Supreme Court, while hearing the Aadhaar-case in Justice KS Puttaswamy vs Indian Govt, recognises right to privacy as a fundamental right; orders govt to introduce relevant lawJustice Srikrishna Committee on data protection constituted |
| July 2018 | <ul style="list-style-type: none">MeitY releases Justice Srikrishna Committee report and proposed draft Bill |
| December 2019 | <ul style="list-style-type: none">Revised Personal Data Protection Bill introduced in Lok SabhaThe Bill referred to Joint Parliamentary Committee (JPC) |
| December 2021 | <ul style="list-style-type: none">JPC submits its report along with a new draft Bill — PDP Bill 2021 |
| August 2022 | <ul style="list-style-type: none">The Indian Govt withdraws the draft PDP Bill 2021 from Lok Sabha |
| Nov 2022 | <ul style="list-style-type: none">MeitY releases a fresh new draft called DPDP Bill, 2022 for public consultation |
| August 2023 | <ul style="list-style-type: none">Govt introduces DPDP Bill 2023 in Lok SabhaParliament enacts the Bill |

Data Protection Board, relevant rules likely in a month

The first set of necessary rules under the Act will be issued within 30 days, said minister Rajeev Chandrasekhar



- Data Management process
- Usage and Sharing process
- Data Control process

- Representation of fact, concepts
- in a manner suitable for communication / processing
- Human / automated means
- Agnostic to medium or format used to convey

Processing of Digital Personal Data

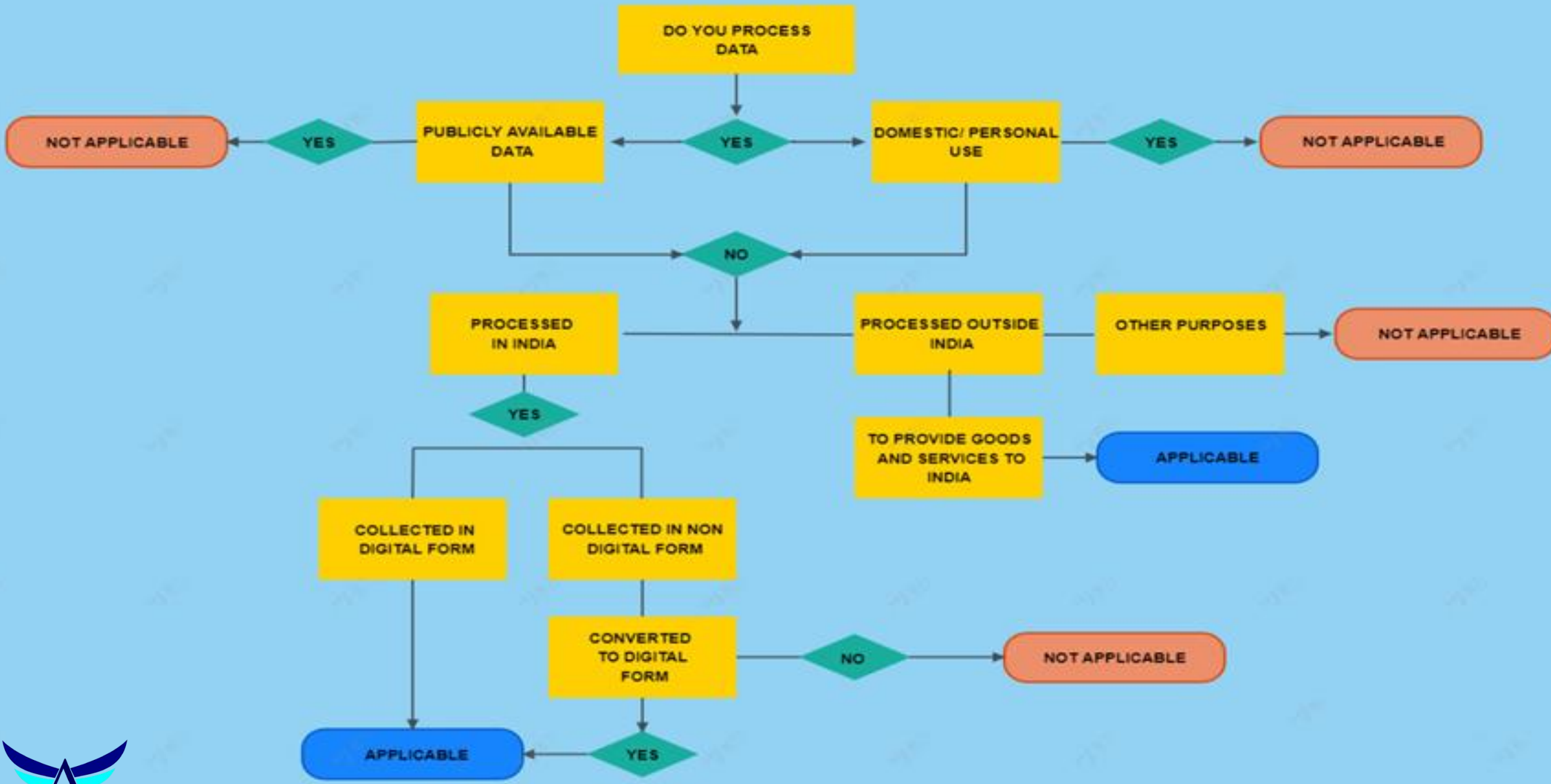
Personal Data, in Digital form

- Data about individuals
- Identifiable by / in relation to such Data

Data Fiduciary

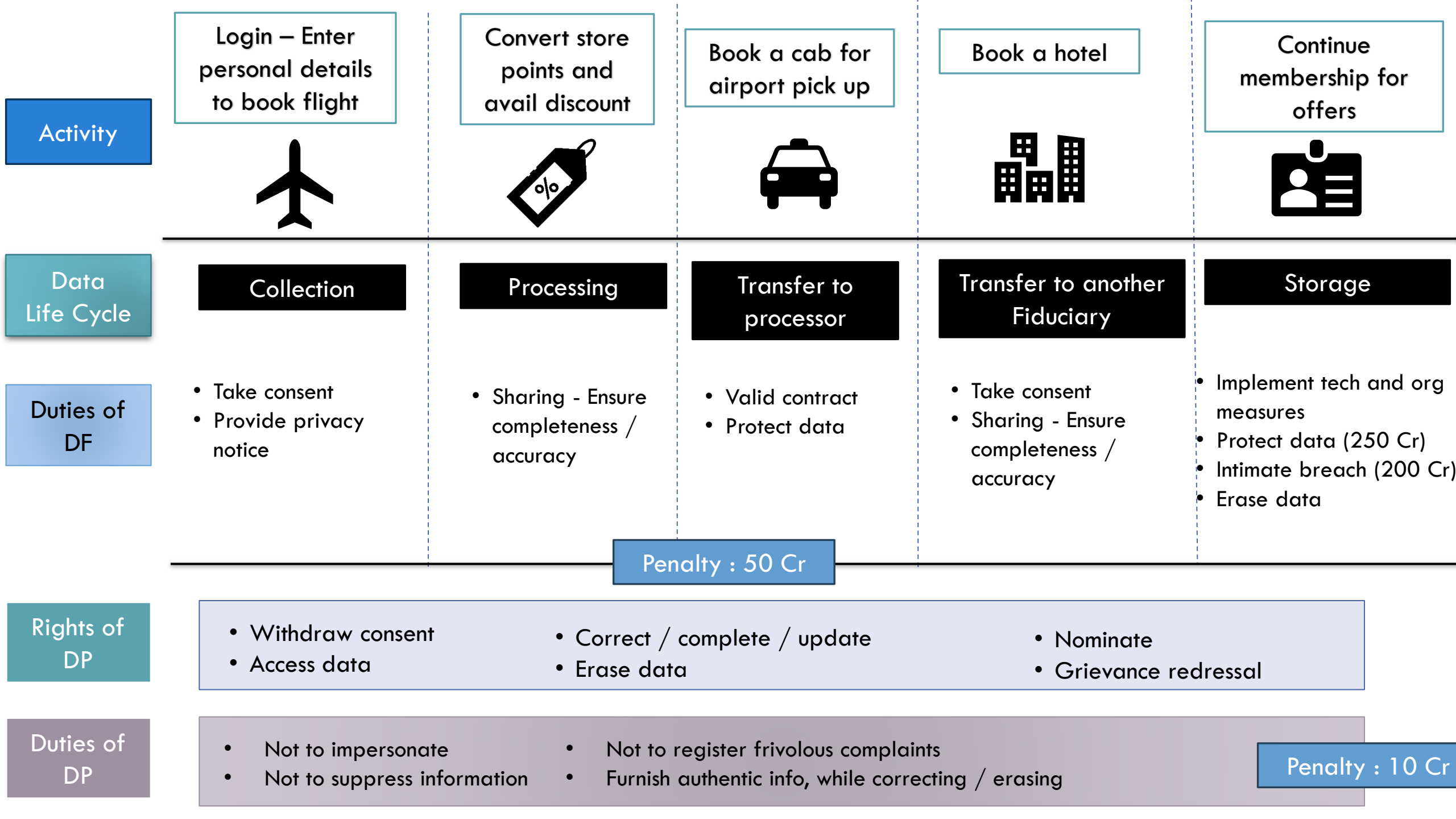
Data Principal

KEY DEFINITIONS



OBLIGATIONS OF DATA FIDUCIARY

1. Obtain Consent. Provide notice
2. Engage a Data processor only under a valid contract
3. Ensure completeness, accuracy of the data
4. implement appropriate technical and organizational measures
5. Protect data in its possession and of the data processed by data processor
6. Personal Data breach - intimate the Board
7. Unless retention is necessary for compliance with law, Erase data
8. Give access to information on the request of DP
9. Correct / erase data on the request of DP
10. Grievance redressal for DP



SPECIAL PROVISIONS

Cross Border Processing

- Government would notify black listed entities
- Stricter law which provides for higher degree of protection (than under DPDPA) will prevail

Exempted processing

- For enforcing Legal Right / Claim
- By judicial and quasi judicial bodies
- For investigation of contravention of law
- For Scheme of arrangement, approved by Tribunal or court
- For ascertaining financial information in the cases of default – IBC

Exempted Persons

- Government entities - to be notified
- Startups – to be notified – based on volume and nature of data
- Other classes of entities – exempted for specified period – to be notified

DATA PROTECTION BOARD

- **Data Protection Board of India - Powers and Functions of the Board:**
 - Handling data breaches
 - Investigating complaints
 - Regulating consent managers
 - Conducting Inquiries and Hearings
- **Voluntary Undertaking:** DPB may accept a voluntary undertaking from an entity, outlining actions to address compliance issues, subject to penalties if not followed.
- **Appellate tribunal - Telecom Disputes Settlement and Appellate Tribunal**
- **Bar of Jurisdiction:** Civil courts are barred from entertaining matters within the purview of DPB
- **Alternate Dispute Resolution:** Option for mediation to resolve complaints, promoting a non-adversarial approach to dispute resolution.

COMPLIANCE PROGRAM FOR DPDPA



INDUSTRIES WHICH BE IMPACTED

- Healthcare institutions
- NBFCs / Fintechs / Account Aggregators / Payment aggregators
- Ecommerce / Retail
- Travel and hospitality
- Marketing and advertising
- Telecom
- Non-Profit organizations
- Tech companies – Big Data, AI focussed.

OPPORTUNITIES

- Acting as a Data Protection Officer
- Drafting of Various policies and documents
- Undertaking Data Privacy Impact Assessment, Data privacy compliance Audit
- Implementing privacy programs
- Evaluate the existing data protection framework and identify areas of non or partial compliance and rectify any issues
- Taking training and awareness programs



Microsoft Excel
Worksheet

FIDUCIARY VS PROCESSOR

- “Data Fiduciary” means any person who alone or in conjunction with other persons **determines the purpose and means of processing** of personal data;
- Hospitals – Labs, NBFCs – Business Correspondents.
- *Data Fiduciary has to comply with all the obligations.*

- Data Processor” means any person who **processes personal data** on behalf of a Data Fiduciary
- E.g. Pay Roll Administration, Website Hosting services
- *No obligations on Data Processors. Will be governed by contract.*

- Joint Fiduciaries
 - E.g-Collaborative assignment, marketing campaigns etc.,
 - Each Data Fiduciary has to comply with all the obligations.

- Significant Data Fiduciary

SIGNIFICANT DATA FIDUCIARY

- To be classified based on the volume and the sensitiveness of data processed

Additional Obligations

- Appoint a Data Protection Officer
- Do Data Protection Impact assessment
- Appoint a Data auditor for independent data audit

1. Data Processor's Indemnity:

1.1 Breach of Data Protection Laws: The Data Processor shall indemnify, defend, and hold harmless the Data Fiduciary against any claims, actions, proceedings, losses, damages, liabilities, costs, and expenses (including reasonable attorney's fees) arising out of or in connection with any breach of this Agreement, Digital Personal Data Protection Act, 2023 (DPDPA), by the Data Processor, its employees, agents, or subcontractors.

1.2 Unauthorized Access or Data Breach: The Data Processor shall indemnify, defend, and hold harmless the Data Fiduciary against any claims, actions, proceedings, losses, damages, liabilities, costs, and expenses (including reasonable attorney's fees) arising from unauthorized access to or acquisition of Personal Data processed under this Agreement or a data breach resulting from the negligence or intentional misconduct of the Data Processor, its employees, agents, or subcontractors.

1.3 Inadequate Security Measures: The Data Processor shall indemnify, defend, and hold harmless the Data Fiduciary against any claims, actions, proceedings, losses, damages, liabilities, costs, and expenses (including reasonable attorney's fees) arising due to the Data Processor's failure to implement and maintain adequate technical and organizational measures as required by the DPDPA, resulting in the compromise of the security and confidentiality of Personal Data.



GROUNDS FOR PROCESSING

```
graph TD; A[GROUNDS FOR PROCESSING] --> B[Consent]; A --> C[Legitimate Use];
```

Consent

Legitimate Use

Consent

- Free, specific, informed, unconditional and unambiguous **with a clear affirmative action.**
- For **specified purpose** and **limited to data necessary** for specified purpose.
- Every request for consent
 - *Plain language*
 - *Option to access in 23 language*
 - *Contact details of Data Protection officer*
- Consent withdrawal - ease of withdrawal
 - Withdrawal will not affect processing before the withdrawal.
 - DF to cause its processor to cease processing
- Data Fiduciary to maintain proof that
 - *Notice was given*
 - *Consent was provided*

Privacy Notice

- Request for consent must be accompanied or preceded by a notice
- Notice to contain
 - *Personal data and purpose for which the same is proposed to be processed*
 - *Process to withdraw the consent*
 - *Grievance redressal process*
 - *Process to complaint to the board*
- Consent taken before commencement of the Act, notice to be given
- Give option to access in 23 languages

LEGITIMATE USE

- Voluntarily provided data for specified purpose
- For the purpose of:
 - Employment
 - Safeguarding the employer from loss or liability,
 - Provisioning any service or benefit sought by employee
- State
 - For the benefits by the state
 - For integrity and sovereignty
 - For fulfilling obligations to disclose to state
- For compliance with any decree or order India or claims contractual or civil nature
- Responding to medical emergencies. Providing medical treatment and health services during epidemic. Taking measures during disaster

- Recruiting process / Background check
- Off-roll employees, contract labours
- Marketing efforts – LinkedIn, YouTube
- After termination / resignation

A TYPICAL PRIVACY NOTICE

- **What information do we collect about you?**
- **How will we use the information about you?**
- **Who do we share your information with?**
- **Where do we process your information?**
- **How long do we keep hold of your information?**
- **How can I withdraw my consent?**
- **How can I exercise my rights?**

- ✓ **Plain and simple language**
- ✓ **Concise**
- ✓ **Layered**
- ✓ **Transparent**



**LAWFULNESS,
FAIRNESS AND
TRANSPARENCY**



**PURPOSE
LIMITATION**



**DATA
MINIMISATION**



ACCURACY



**STORAGE
LIMITATION**



**INTEGRITY AND
CONFIDENTIALITY**



ACCOUNTABILITY

PRINCIPLES OF PROCESSING

TECHNICAL AND ORGANISATIONAL MEASURES

Technical

- ✓ Focus on the technological aspects of data security and privacy
- ✓ Tools to safeguard data

- Encryption
- Access Control
- Data Minimization
- Data Masking and Psuedonymization
- Data Portability
- Secure Development
- Regular Updates and Patch Management
- Data Loss Prevention (DLP)
- Secure Communication

Organizational

- ✓ Focus on the policies, procedures, and practices
- ✓ Revolve around human and administrative aspects of data protection

- Impact assessment
- Audits
- Policies and process
- Employee trainings
- Privacy by design
 - User friendly interface
 - Data minization
 - Transparency

POLICIES

1. Cookie Policy
2. Third Party data processing policy
3. Data Retention Policy
4. Employee monitoring policy
5. Data Breach Response and Notification Procedure
6. Data Principal Rights response procedure
7. Grievance Redressal mechanism
8. Website terms and conditions

| Functions | Data / Activity impacted |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Human Resources | Recruitment, Off roll employees, Employee monitoring, post resignation, Outsourcing of payroll activities, Employee records |
| Secretarial | Directors' data Investor data CSR data |
| Finance and Accounts | Invoicing, billing, Payment processing Audit – Statutory / Internal |
| Legal | Legal Claims / petitions Compliance reporting |
| Credit | Personal details of the Creditors Risk assessment / Credit Score reports |

| Functions | Data / Activity impacted |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Sales and Marketing | Usage of customer data for marketing Leads and referrals. Marketing campaigns |
| Information Technology | Security features Usage of emails and data storage in private instruments of employees. Cookies, terms of use of website |
| Social media | Poll Results, Data Analytics, influencer colorations |
| Administration | Video surveillance, Employee events, any outsourcing activities |



Flat No.7, Door No.10 Madhans, South Canal
Bank Road, Mandavelipakkam, Chennai
600028

Phone: [044-4353 3080](tel:044-43533080)

bhuvana.r@akshayamcorporate.com
Jayanth.v@akshayamcorporate.com



R Raja Krishnan, Head – Legal
Akshayam Corporate Advisors Private
Limited

Phone : 93 8020 7585

raja.Krishnan@akshayamcorporate.com





THANK YOU |