# Digital Personal Data Protection Act (2023), India

## Applicability of the law

- Processing of personal data in digital format within the territory of India and outside India
- Processing of non- digital personal data that was subsequently digitised
- Processing of personal data, whether within the Indian territory or outside India, for the systematic activity of offering goods and services to data principals within India

- Processing for domestic or personal purposes by individuals
- Personal data made publicly available.

## Key Definition

**Data Principal**
An individual to whom the personal data relates to including a child, a person with disability, and their lawful guardian acting on their behalf.

**Data Fiduciary**
Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data

**Significant Data Fiduciary (SDF)**
SDF will be identified by the Central Government using the volume and sensitivity of personal data processed (among other criteria) and risk associated

**Data Processor**
Any person who processes personal data on behalf of a Data Fiduciary

## Obligations of Data Fiduciaries

- Provide a clear, concise and comprehensible notice to data principals
- Ensure data collected is accurate, complete and consistent
- Process personal data for which data principal has given consent or for certain legitimate uses
- Report Personal Data Breaches to Data Protection Board and Data Principals
- Erase their personal data unless retention of the same is necessary
- Implement technical and organizational measures to ensure effective adherence with the law

## Journey to Compliance*

1. Undertake a Data Privacy Assessment to understand the current posture toward privacy and the requirements
2. Develop a data privacy framework to strengthen your organizations data privacy program
3. Establish the Data Privacy Organization to drive the program
4. Data Discovery, Classification, and Mapping exercise to identify the personal data touch points, and structured and unstructured data across the environment and classify them
5. Develop an inventory of assets processing personal information and also the entire list of suppliers / 3rd parties leveraged for various purposes / delivering the services
6. Develop/update relevant policies and underlying procedures to outlay the intent and consistent approach toward privacy and protection
7. Conduct Data Privacy Impact Assessments (DPIAs) for the high-risk in-scope business functions/ applications to identify the potential risk exposure
8. Establish mechanisms for Consent management, Data principal rights and Breach notification
9. Implement Privacy Enabling Technologies (PETs) to reduce manual task

*EY can support organizations across the phases of the Journey to Compliance

## Key Highlights of the law

**Notice** - Provide clear, itemised notice in simple language that includes purpose and manners of accessing rights and make complaints.

**Grounds of Personal Data Processing:**
1.Legitimate Uses
2.Consent

**Data Principal Rights**- Right to information, Right to grievance redressal*, Right to correction and erasure and Right to nominate (* Timeline to respond shall be notified by the central government)

**Transfer of Personal Data outside India**- The Central govt. to notify such countries or territories outside India to which a Data Fiduciary may not transfer personal data

**Legitimate Uses**
**Consent is not expressly needed for situations such as :**
Voluntary disclosure by the data principal, Reasonable expectation by the data principal, Medical emergency among others, Threat to public health, and ensuring safety in case of any disaster

**Non-reporting of breaches** - The liability for not reporting breaches or failing to institute safeguards falls on data fiduciaries.

**Children's Data** - Obtain verifiable parental consent before processing any personal data related to children.

**Data Protection Board of India** - The Central Government may, by notification appoint and establish, an independent Board to be called the Data Protection Board of India.

### Data Principal Duties

- Comply with provisions of law
- Do not impersonate another person
- Do not supress any material information
- Do not register false and frivolous compliant
- Furnish only verifiably authentic information

### Obligations of SDFs*

- Appoint a DPO based out of India
- Perform DPIAs
- Appoint an independent data auditor
- Perform periodic audits

*Significant Data Fiduciaries

**Consent** - Organizations must obtain clear, informed, and unambiguous consent from Data Principals through a distinct affirmative action.

**Consent Manager**- The Data Principal can grant, control, review, or revoke consent to the Data Fiduciary using a Consent Manager, which must be registered with the board.

### Penalties

**Up to ₹ 250 Crores**
Noncompliance of the provisions by Data Fiduciaries

Up to ₹ 200 Crores
Breach in observance of additional obligation in relation to children

**Up to ₹ 10 Thousand**
Breach in observance of duty of Data Principal

**Up to ₹ 200 Crores**
Breach in not giving notice of personal breach

EY has 100+ certified CIPPs/CIPM/CIPT from IAPP globally

EY is platinum partner of the International Association of Privacy Professionals (IAPP)

EY is actively involved with the Data Security Council of India (DSCI) in helping them in various initiatives

EY has an extensive network of privacy SMEs having experience on 35+ personal data protection regulations

EY has published thought leaderships and articles in association with leading organizations such as ASSOCHAM etc.

Ernst & Young LLP
EY | Building a better working world



ED None
EYIN2309-004