DIGITAL PERSONAL DATA PROTECTION LAW

Over the years, India has seen various iterations of a draft data protection law. In August 2023, the Digital Personal Data Protection Act, 2023 ("DPDPA") was passed by the Indian parliament. The Digital Personal Data Protection Act of Parliament received the assent of the President on the 11th August, 2023.

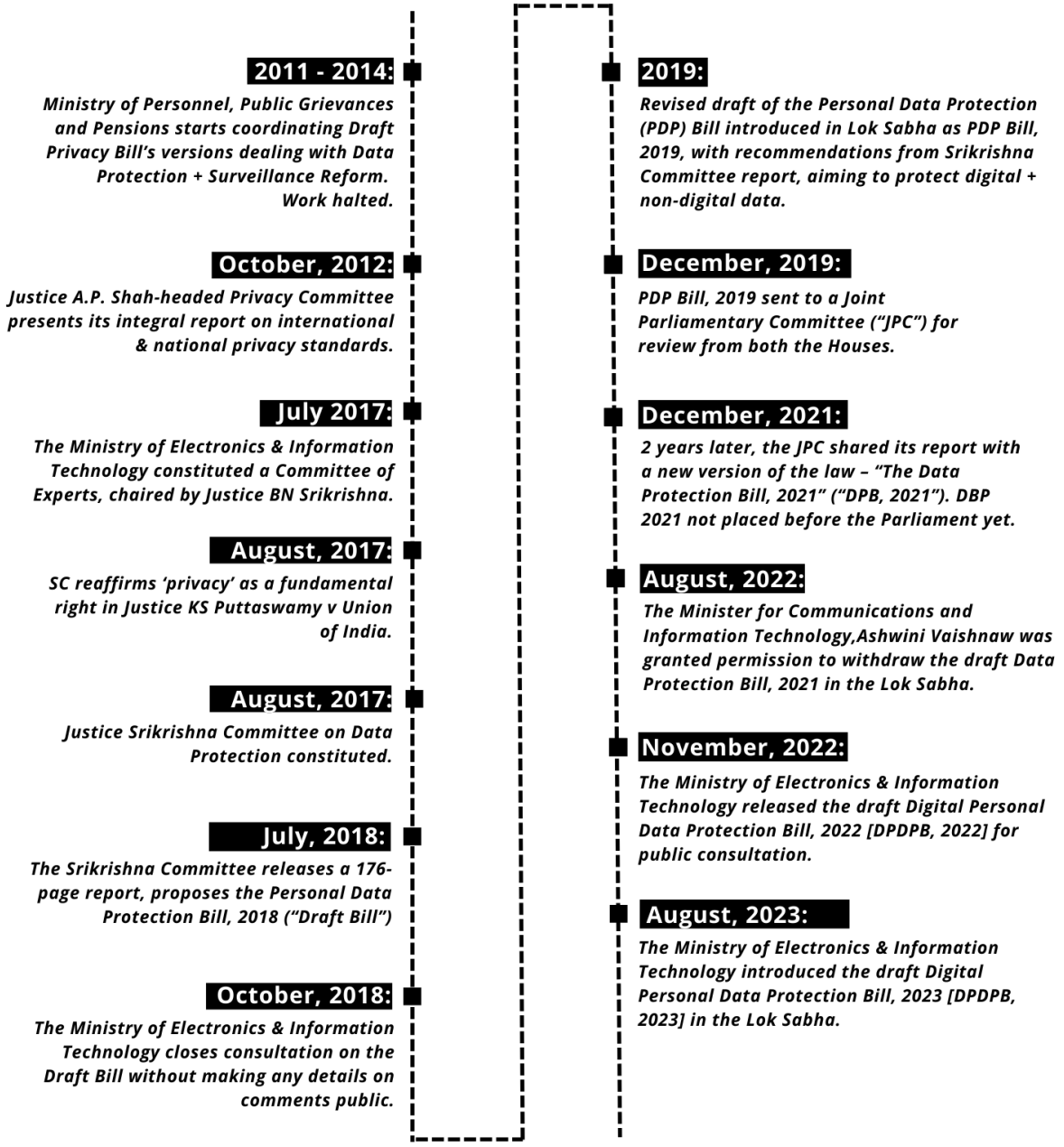
Introduction

"Data is the new oil." It signifies that data is a valuable asset that is being explored by businessmen in order to extract huge profits. It is naturally unrefined and needs to be converted into something of value. Also, we are now a part of the digital economy, where every person is reduced to data. Data is better than opinions; it is preferred as it is more reliable and predictable. We can predict outcomes based on existing data, get insights for better business performance, make better strategies, etc. But it can be equally disastrous if the data is not handled with care. Data is indeed powerful on its own, but it needs the aid of the law to be regulated. Thus come data protection and privacy laws.

In this era where digital information flows across borders within seconds, the evolution of data protection laws in India has become an important point of discussion among policymakers, businesses, and citizens. The need to protect people's privacy from misuse or unauthorized access stands out now more than ever given how fast services are increasingly being digitized resulting in rising concerns over data security and individual rights to privacy in this country. With the evolution of the Indian data privacy laws for addressing these issues, it becomes necessary for all stakeholders involved to understand the landscape of personal data protection in India, its current state, and its future direction.

The development and implementation of the data protection bill in India signal the country's commitment to establishing a robust legal framework that aligns with global standards such as the General Data Protection Regulation (GDPR) of the European Union, highlighting its importance on the international stage. Like many data privacy laws around the world, the DPDP Act is extraterritorial, and so applies to organizations operating both inside and outside of India, if they are offering goods or services to Indian citizens, and in doing so processing personal data. The Act does allow for legal bases for data processing in addition to consent of the data principal, but consent is required for many processing purposes. The Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant milestone in India's journey towards safeguarding individual privacy in the digital age.

Data Protection Framework Timeline



Historical Background

In India, the concept of Data protection has evolved significantly over the past decade. Initially, the Information Technology Act of 2000, along with its amendment in 2008, laid the groundwork

by addressing information security rather than comprehensive data protection. Moreover, the concept of data protection and privacy has been debated in the judicial courts with some addressing it as a fundamental right. In contrast, others were not admitting it as a right under Article 21 of the Indian Constitution. The landmark judgment of the top Court in *Justice K.S. Puttaswamy (Retd.) & Ors. v. Union of India in 2017*, recognizing the right to privacy as a fundamental right, accelerated legislative efforts. This led to the drafting of the data protection bill, resulting in the introduction of the Digital Personal Data Protection Act of 2023.

Current Scenario in Data Protection Law in India

The Digital Personal Data Protection Act, 2023 (DPDPA), marks a significant milestone as India's first comprehensive legislation on data protection. This Act regulates the collection, use, and disclosure of personal data. Until this Act is fully operational, the Information Technology Act, 2000 (IT Act), and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, continue to govern the Indian data protection framework.

Section 43A of the IT Act deals with 'Compensation for failure to protect data'. It states that "Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected."

Section 72A of the IT Act deals with 'Punishment for disclosure of information in breach of lawful contract'. As per this Section, any person including an intermediary who, while providing services under the terms of a lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses such material to any other person, without the consent of the person concerned or in breach of a lawful contract should be punished with imprisonment for a term which may extend to 3 years, or with fine which may extend to 5 lakh rupees (5,00,000), or with both.

Need

- ✓ **Data as the New Oil:** With the rapid growth of India's data economy, regulating the rich data shared by Indians daily on various platforms is crucial, whether for banking, shopping, or social media.
- ✓ **Threats to the Digital Economy:** The pandemic has exponentially increased risk exposure to the digital economy, exemplified by incidents like ransomware attacks and data breaches at companies like Mobikwik.
- ✓ **Internet Crime:** A robust data protection regime is essential to safeguard against internet crimes such as cybercrime, cyberbullying, and harassment.
- ✓ **National Security Concern:** The data of security agencies could be at risk, compromising national security, and there is resistance to data localization from private entities.
- ✓ **Surveillance State:** Inadequate data protection laws can lead to unrestricted government access, potentially fostering a totalitarian regime, as seen with the Aadhar Act.
- ✓ **Currently**, personal data is regulated by the IT Act, 2000, applicable only to foreign companies and corporates in India.
- ✓ **Puttaswamy Case (2017):** The Supreme Court declared data privacy a Fundamental Right under Article 21.

Key definitions in the Indian Personal Data Privacy Law

The definitions of key terms outlined in the DPDP Act are consistent with many data privacy laws, though some of the terms are different, e.g. "data fiduciary" instead of "data controller". The definition of a person is also quite broad, as it can include the Indian State, a family, or a firm, for example.

What is a person under the DPDP Act?

A person covers a variety of entities, not just individual people, and refers to:

- ✓ an individual
- ✓ a Hindu undivided family
- ✓ a company
- ✓ a firm
- ✓ an association of persons or a body of individuals, whether incorporated or not
- ✓ the State
- ✓ every artificial juristic person, not falling within any of the preceding sub-clauses

What is personal data under the DPDP Act?

- ✓ Personal data refers to any data about an individual who is identifiable by or in relation to such data. The personal data can be collected and processed in digital format, or collected in another format and later digitized. The Act does not provide a list of examples of personal data (e.g. name, phone number, financial information, etc.) like some data privacy laws do.

What is processing under the DPDP Act?

- ✓ Processing in the context of personal data means "a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction".

What is the definition of consent under the DPDP Act?

- ✓ A data principal's consent must be: "free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose".

Who is defined as a child under the DPDP Act?

- ✓ A child is defined as a person who is 18 years old or younger.

Who is a data principal under the DPDP Act?

- ✓ This term refers to any individual to whom personal data being processed relates, and includes an individual who is a child (also, then, including the child's parents or lawful guardians) or an individual who has a disability (also, then, including the person's lawful guardian, acting on their behalf). Also known as a data subject under some other laws.

Who is a data fiduciary under the DPDP Act?

- ✓ "Data fiduciary" means any person who, alone or in conjunction with other persons, determines the purpose and means of processing of personal data. Also known as a data controller under some other laws.
- ✓ A "Significant Data Fiduciary" refers to any data fiduciary or class of data fiduciaries as may be notified by the Central Government.

Who is a data processor under the DPDP Act?

- ✓ A data processor is any person who processes personal data on behalf of a data fiduciary.

What is a consent manager under the DPDP Act?

- ✓ For the purposes of the Act, "Consent Manager" does not refer to software such as a consent management platform, but instead refers to a person or organization registered with the Data Protection Board. This entity acts as the point of contact to enable an individual, here the "data principal", to provide, manage, review, and/or withdraw her consent via a platform that is "accessible, transparent and interoperable". A consent manager serves as a middleman for businesses to help facilitate compliance with the DPDP Act.

Key Provisions of the Act

- ✓ **Applicability:** The act applies to the processing of digital personal data within India, whether collected online or offline and digitized. It also applies to the processing of personal data outside India if it involves offering goods or services in India.
- ✓ **Consent:** Personal data can only be processed for lawful purposes after obtaining the individual's consent. A notice must be given before seeking consent, detailing the personal data to be collected and the purpose of processing.
- ✓ **Lower Age of Consent:** The act allows the central government to prescribe a lower age of consent than 18 years for accessing internet services without parental consent if the platform processes their data safely. This benefits sectors like edtech and medical services.
- ✓ **Ease of Cross-Border Data Flows:** The act facilitates cross-border data flows by adopting a blacklisting mechanism instead of a whitelisting approach.
- ✓ **Impact on Social Media Companies:** Significant Data Fiduciaries must develop user verification mechanisms, reducing anonymity, trolling, fake news, and cyberbullying.
- ✓ **Exemptions:** Certain cases are exempt from the rights of data principals and obligations of data fiduciaries (except data security). These include prevention and investigation of offenses and enforcement of legal rights or claims. The central government may exempt activities like processing by government entities for state security and public order.
- ✓ **Data Protection Board of India:** The central government will establish this board to monitor compliance, impose penalties, direct necessary measures in data breach events, and

hear grievances. Board members will be appointed for two years with eligibility for reappointment.

- ✓ **Penalties:** The act specifies penalties for various offenses, such as up to Rs.200 crore for failing obligations to children and Rs.250 crore for failing to prevent data breaches. Penalties are imposed after an inquiry by the Board.

Significance

- ✓ **Efficient Crime Investigation:** With data stored within national borders, law enforcement agencies can efficiently investigate crimes, ranging from financial fraud to cybercrime, without bureaucratic hurdles.
- ✓ **Protection from Cyber Attacks:** High-profile cases like the WhatsApp hack by Pegasus highlight the vulnerability of data stored overseas. Data localization ensures better control and protection against such cyber threats.
- ✓ Keeping data within national borders can reduce the risk of ransomware attacks, as local authorities can respond more effectively to such incidents.
- ✓ **Empowerment of Individuals:** The Data Protection Act empowers individuals with greater control over their personal data through rights such as consent for data processing, correction of inaccurate data, and grievance redressal mechanisms.
- ✓ **Enhanced Transparency:** The Act mandates transparency from data fiduciaries regarding the collection, use, and processing of personal data, building trust between individuals and data-handling entities.
- ✓ **Data Minimization Principle:** The Act emphasizes the principle of data minimization, requiring that only data necessary for a specific purpose be collected and processed, thereby reducing the risk of data misuse.
- ✓ **Obligations for Data Fiduciaries:** Data fiduciaries are required to implement strong data security measures, conduct data protection impact assessments, and ensure compliance with data protection principles, thereby enhancing overall data security.
- ✓ **Data Protection Board of India:** The establishment of the Data Protection Board of India ensures a dedicated authority for monitoring compliance, investigating breaches, and adjudicating disputes, contributing to a more regulated data protection environment.
- ✓ **International Data Transfers:** The Act regulates cross-border data transfers, ensuring that data transferred outside India is afforded adequate protection, thus safeguarding the privacy of Indian citizens.
- ✓ **Addressing Emerging Technologies:** The Act provides a framework to address data protection challenges posed by emerging technologies like artificial intelligence, ensuring that data processing in these domains adheres to privacy principles.
- ✓ **Promoting Digital Economy:** By establishing a secure data protection regime, the Act promotes confidence in the digital economy, encouraging more businesses and individuals to engage in digital transactions and services.
- ✓ **Alignment with Global Standards:** The Act aligns India's data protection framework with global standards, such as the GDPR, facilitating smoother international business operations and data exchanges.

Data Privacy Law in Other Countries

An overview of data privacy law in other countries includes:

- ✓ **European Union:** In 2018, **General Data Protection Regulation (GDPR)** came into effect. It is a comprehensive law that was formed to imposes strict rules on the collection and processing of personal data especially by businesses and organizations.
- ✓ **Japan:** To governs personal data **Act on the Protection of Personal Information (APPI)** is present. It requires consent of the user and provides for various security measures.
- ✓ **China:** In China, the right to prevent the misuse of personal data is present under **The Personal Information Protection Law (PIPL)**.
- ✓ **Australia:** Private individual data is governed under Privacy Act.
- ✓ **South Africa:** Individual information is protected under **Protection of Personal Information Act (POPIA)**.

DPDP Act vs GDPR

Comparing the Digital Personal Data Protection Act 2023 (DPDP Act) with the General Data Protection Regulation (GDPR) reveals both similarities and distinctions:

- ✓ **Scope and Application:** While the GDPR is a regulation across the European Union, the DPDP Act is specific to India, each with its territorial applicability and global reach for companies dealing with respective citizens' data.
- ✓ **Consent:** Both laws emphasize the importance of obtaining clear and informed consent for data processing, but the GDPR has stricter requirements for consent validity.
- ✓ **Data Protection Officer (DPO):** The appointment of a DPO is mandatory under GDPR for certain organizations, whereas the DPDP Act also suggests appointing a data protection officer depending on the volume and sensitivity of data processed.

Concerns

Exemptions to the State and Privacy Implications

- ✓ **Broad Exemptions:** Personal data processing by the State includes central and state governments, local bodies, and government-set-up authorities and companies. These exemptions can enable unchecked data processing by the State.
- ✓ **Violation of Right to Privacy:** Exemptions may lead to excessive data collection, processing, and retention, violating the right to privacy. The Supreme Court's proportionality principle from the 2017 Puttaswamy case requires any privacy infringement to be necessary and proportional.
- ✓ **Unchecked Data Processing:** The Bill allows the central government to exempt government agencies from provisions for state security and public order. This can lead to data being collected and used without purpose limitation, potentially violating privacy.
- ✓ **Lack of Deletion Requirement:** Government agencies are not required to delete personal data after the purpose for processing is met, raising concerns about surveillance and profiling.
- ✓ **Proportionality Test:** Similar to UK laws, which include safeguards like necessity and proportionality for data processing, India's act lacks such robust oversight mechanisms.

Overriding Consent for State Purposes

- ✓ **Consent Override:** The act allows the State to override individual consent for

providing benefits, services, licenses, permits, or certificates, removing purpose limitation. Combining data for various purposes can lead to citizen profiling. Requiring consent would give individuals more control over their personal data.

Regulation of Harm from Data Processing

- ✓ **Lack of Harm Regulation:** The act does not address risks of harm from data processing, such as financial loss, identity theft, discrimination, and unreasonable surveillance.
- ✓ **Srikrishna Committee Recommendations:** The Committee recommended regulating harm under data protection law and providing compensation for affected individuals, similar to the European GDPR.

Right to Data Portability and Right to be Forgotten

- ✓ The act does not provide for the right to data portability or the right to be forgotten, which were included in earlier drafts and are recognized by GDPR.
- ✓ **Data Portability:** This right allows individuals to transfer their data in a structured, machine-readable format, enhancing control over personal data.
- ✓ **Right to be Forgotten:** This right limits the disclosure of personal data on the internet, balancing privacy with other rights like free speech.

Cross-Border Data Transfer

- ✓ **Adequacy of Protection:** The act allows unrestricted data transfer to all countries except those specifically restricted, raising concerns about data protection standards in other countries.
- ✓ **Selective Restriction Mechanism:** Unlike exhaustive evaluations required in previous drafts, the current Bill's selective restriction mechanism may not ensure adequate protection.

Independence of the Data Protection Board

- ✓ **Short Appointment Term:** Members of the Data Protection Board are appointed for two years with reappointment eligibility, which may affect their independence.
- ✓ **Executive Influence:** Short terms with reappointment increase executive influence and control, impacting the Board's ability to monitor compliance, conduct investigations, and adjudicate penalties independently.
- ✓ **Comparison with Other Regulatory Bodies:** Regulatory bodies like the Central Electricity Regulatory Commission and the Competition Commission of India have longer appointment terms (five years), promoting independence.

Way Ahead

- ✓ **Regular Updates:** Ensure the legal framework is regularly updated to keep pace with technological advancements and emerging data protection challenges.
- ✓ **Independent Oversight:** Strengthen the independence and authority of the Data Protection Board of India to ensure impartial enforcement and adjudication of data protection laws.
- ✓ **Incentives for Compliance:** Provide incentives for companies to comply with data localization requirements, such as tax breaks or subsidies for building local data centers.
- ✓ **Strengthen Local Infrastructure:** Invest in developing robust local data storage and

processing infrastructure to support data localization efforts and ensure data security.

- ✓ **Balance with Global Operations:** Implement data localization policies that balance national security concerns with the needs of businesses operating internationally, facilitating smooth cross-border data transfers where necessary.
- ✓ **Awareness Campaigns:** Conduct nationwide awareness campaigns to educate individuals about their data protection rights and how to exercise them
- ✓ **User-Friendly Mechanisms:** Develop user-friendly mechanisms for individuals to access, correct, and delete their personal data, enhancing their control over their data.
- ✓ **Foster Data-Driven Innovation:** Encourage data-driven innovation by creating a regulatory environment that supports the responsible use of data, balancing privacy concerns with the benefits of data analytics and Al.
- ✓ **International Cooperation:** Promote international cooperation on data protection to facilitate global business operations, ensuring that Indian businesses can compete effectively in the global market while adhering to stringent data protection standards.

Conclusion

The Data Protection Act 2023 represents a significant step towards **enhancing data privacy** in an increasingly data-driven world. By establishing clear rules and responsibilities for data handling, it aims to build trust in the digital ecosystem and protect personal information effectively.