

Ensuring Compliance with the Indian Digital Personal Data Protection Act Using Seclore Data-Centric Security



SECLORE™

Ensuring Compliance with the Indian Digital Personal Data Protection Act Using Seclore Data-Centric Security

The Indian DPDP Act is India's first data protection bill, passed in August 2023 after a decade of deliberation. The DPDP Act regulates the collection, use, and processing of personal data by businesses and organizations in India. The aim is to protect individuals' personal information and ensure fair and transparent collection and usage. This goal involves two key aspects: maintaining privacy and promoting clarity.

The Act defines personal data and sensitive personal data. It limits how organizations collect, use, and process data, requiring consent and disclosure of purpose. The Data Protection Authority enforces the law, investigating complaints and imposing breach penalties.

This whitepaper shows how Seclore can assist organizations in following the DPDP Act to protect and manage consumer personal information effectively.

Scope of the Indian Digital Personal Data Protection Act

The Indian Digital Personal Data Protection (DPDP) Act aims to balance privacy rights and lawful use of data, enabling organizations to access and apply data for business purposes while safeguarding people's privacy and promoting digital innovation.

The scope of the Act covers the following seven principles:

- **Transparency:** Consented, lawful, and transparent use of personal data.
- **Purpose limitation:** Use personal data only for the specified purpose when obtaining the Data Principal's consent.
- **Data minimization:** Collecting as much personal data as necessary to serve the specified purpose.
- **Data accuracy:** Ensuring data is correct and updated.
- **Storage limitation:** Storing data only till needed for the specified purpose.
- **Data security:** Reasonable security safeguards.
- **Accountability:** Through adjudication of data breaches and breaches of the provisions of the Act and imposition of penalties for the breaches.



Unlocking DPDP Compliance with Data-Centric Security

As an organization, you understand the importance of safeguarding your data. One effective method to achieve this is through data-centric security. Simply put, the data-centric approach allows you to determine who can access your sensitive information. This helps to build trust with your clients since only authorized personnel can view it.

Additionally, you can limit data usage to specific purposes as long as you have obtained consent. To maintain privacy, you can dispose of unnecessary data. With a reliable data protection plan, you can comply with regulations and ensure the safety of your business.

How Does Data-Centric Security Help Comply with the Indian DPDP Act 2023

The data-centric security approach provides highly dependable security that prioritizes data protection. Data-centric security ensures complete privacy by precisely controlling data access and distribution, focusing on data. This implies that only authorized personnel can access and utilize personal data.

An efficient data-centric security platform utilizes a centralized logging system to monitor access attempts to data. This system tracks all attempted and authorized access to safeguarded data, generating a transparent trail of information. The trail helps them track attempted access to specific data. It includes important details such as IP address, device name, and file location.

Data Collection:

Organizations can use classification-driven protection to classify their data based on specific keywords. The DPDP Act of India guarantees that we recognize and provide additional security measures for sensitive personal information.

Data-centric security provides secure data collection mechanisms to help with data collection. It also allows users to share sensitive data safely and securely. Authorized users have access permission to protect internal data.

The Data Protection Portal displays user consent messages for data collection. It guarantees the collection of only necessary and authorized data. This is per the Indian DPDP Act.

Impact: Organizations can build customer trust by implementing precise consent management and data collection processes through the Data Protection Portal. Transparency and control over data collection can build customer trust, improve brand reputation, and reduce legal risks.

Data Storage:

Data-centric security can help securely store personal data using encryption and access controls. Under the DPDP Act, data-centric security ensures that sensitive data is encrypted and only accessed by authorized personnel with the lowest usage privileges, helping Indian businesses store data securely and confidentially.

Impact: Data-centric security protects personal data by encrypting it and controlling access. This reduces the risk of data breaches and unauthorized access. It also improves data security and safeguards the organization from potential leaks, financial losses, and damage to its reputation.

Data Usage and Processing:

If third parties need to handle your data, they should sign a non-disclosure agreement (NDA) or use encryption to keep it safe. Data-centric security goes even further by letting organizations enforce the rules in an NDA. This makes the security offered by an NDA more real.

With advanced data-centric security, an NDA provides a complete way to protect data. Encryption, access controls, tracking, and dynamic usage policies help businesses manage and protect their digital assets well.

Data-centric security solutions enable enterprises to enforce personal data use and processing policies. These policies determine who can access and modify data under certain conditions, ensuring compliance with the Indian DPDP Act. Data-centric security enables revoking access to sensitive information and automatically expiring outdated data to eliminate security risks.

Impact: Data-centric security enables organizations to demonstrate responsible data handling. To avoid penalties and comply with the Indian DPDP Act, organizations should have clear policies for using and handling personal data. These policies help prevent the misuse of data and keep it safe.

Data Retention:

Data-centric security measures in classification solutions ensure compliance with legal requirements and minimize personal data retention. Tracking and defining retention periods and deletion schedules within labeled documents becomes more accessible by classifying data. This ensures adherence to provisions on data retention in the Indian DPDP Act.

Impact: Data-centric security assists in efficient and compliant data retention practices. Organizations can avoid unnecessary data hoarding, reduce storage costs, and minimize legal liabilities. Effectively managed data retention also enhances data accuracy and the ability to respond to customer requests promptly.

Data Access Control:

Organizations can utilize data-centric security solutions to manage access to personal data. These solutions incorporate robust access control mechanisms that restrict access based on roles, responsibilities, and authorization levels. This aligns with the efforts of the Indian DPDP Act to ensure that only authorized individuals can access personal data. Furthermore, organizations can grant the least usage privileges to authorized users.

Impact: Data-centric security enhances overall data security, reduces the risk of insider threats and unauthorized data access, and limits the potential for data breaches.

Consent Management:

Data-centric security can help manage user consent by maintaining records of consent obtained from individuals for various data processing activities. This can assist enterprises in demonstrating compliance with the requirements of the Indian DPDP Act for obtaining and managing user consent.

Impact: Implementing robust consent management through data-centric security demonstrates a commitment to respecting individuals' privacy choices. Organizations that handle customer data transparently and according to their preferences are likelier to build strong customer relationships based on trust.

Auditing and Reporting:

Data-centric security includes auditing and reporting features that track and document data access and usage. Enterprises can show that they follow data protection regulations by providing audit trails. This is per the transparency requirements of the Indian DPDP Act.

Impact: A data-centric security auditing and reporting platform helps organizations maintain compliance with the Indian DPDP Act. Keeping accurate and detailed records helps meet regulatory requirements, promotes responsibility, and reduces legal risks in handling data.

Introduction to Seclore Data-Centric Security

Seclore's security platform is designed to protect your digital assets with a data-centric approach, giving you complete control and protection wherever you are. This comprehensive solution fully complies with the Indian DPDP Act, ensuring organizations can maintain compliance through a data-centric security approach. Our approach guarantees the security of your data during transit and storage while keeping track of all access to your data. Seclore provides complete protection for your digital assets, ensuring they are always secure.

Benefits of Using Seclore Data-Centric Security to Comply with the Indian DPDP Act

Organizations can benefit from implementing Seclore's data-centric security solution while fulfilling the responsibilities established in the Indian Digital Personal Data Protection Act 2023. The following are the summarized benefits:

Transparency:

Maintains comprehensive audit trails and automated notifications, enhancing transparency and accountability.

Compliance:

Helps organizations adhere to legal requirements, avoiding penalties and legal consequences.

Risk Mitigation:

Mitigate data breaches, unauthorized access, and other security risks.

User Trust:

Empowers data fiduciary users with control over their data, building trust with individual users and demonstrating positive user experiences.

Reputation:

Demonstrates commitment to data protection, enhancing the organization's reputation.

Resource Optimization:

Optimizes resource allocation by automating processes related to breach notifications and more.

Conclusion

At Seclore, we prioritize data-centric security measures like encryption and dynamic watermarks to protect data throughout its lifecycle. Our security features contribute to integrity, confidentiality, and accountability by preventing unauthorized access and providing detailed audit trails for compliance reporting. Furthermore, our data deletion process is secure and guarantees the protection of personal information.

We understand that running a business is challenging, and protecting your data from attacks is another layer of complexity. Seclore can be a valuable resource for your business. By providing protection, organizations can focus on running their business with the peace of mind that their information is secure.



Annexure: Glossary

Data: "Data" means a representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by human beings or by automated means.

Personal Digital Data: Digital Data about an individual that can identify them, including identifiers like name, phone number, Aadhaar, and PAN.

Children Data: Data of individuals below the age of 18.

Statement: An Act to provide for the processing of digital personal data in a manner that recognizes both **the right of individuals to protect their personal data** and the **need to process such personal data for lawful purposes** and matters connected in addition to that or **incidental to it**.

Intent: Ensure that the processing of digital personal data is done lawfully, ethically, and transparently while simultaneously encouraging innovation and development.

Scope: Whether obtained online or by offline digitization, the DPDP (Digital Personal Data Protection) Bill applies to all digitally processed personal data.

Geography: Includes processing digital personal data on Indian citizens inside and outside Indian territory.

Stakeholders: Data Principal, Data Fiduciaries, Data Processor, Significant Data, Data Protection Board of India

Role of Data Principal: Right to access anytime, right to correction and erasure, right to grievance redressal, right to nominate.

Duties of Data Principal: Follow all laws, no impersonation, share complete and accurate details, and provide authentic information.

Personal Data Breach: Means any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction, or loss of access to personal data that compromises the confidentiality, integrity, or availability of personal data.

Data Fiduciary: means any person who, alone or in conjunction with others, determines the purpose and means of processing personal data.

Obligations of Data Fiduciary: Give notice to the Data Principal, obtain the consent of the data principal, data accuracy and completeness (security measures to prevent data breaches), notify the data breaches, and delete data after the purpose is fulfilled.

Cross Boarder Processing and Transfer: The bill permits the transfer of personal data outside India, except to countries restricted by the government through official notification.



About Seclore

Protecting the world's sensitive data wherever it goes. Seclore protects and controls digital assets to help enterprises close their data security gap to prevent data theft and achieve compliance. Our data-centric approach to security ensures that only authorized individuals have access to sensitive digital assets, inside and outside of their organization. Enterprises can set automated policies and enable users to control and revoke who has access, what access they have, and for how long. Learn why leading enterprises like American Express choose Seclore to protect and control their digital assets without sacrificing seamless collaboration and data sharing.

Visit www.seclore.com for more information.

5201 Great America Parkway
Suite 440
Santa Clara, CA 95054