Compliance Brief

India's DPDPA

Simplifying Compliance with the Digital Personal Data Protection Act and build customer trust

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

The Indian Parliament passed the Digital Personal Data Protection Act (DPDPA), 2023 in August 2023. The DPDPA will replace Section 43A of the Information Technology Act, 2000 ("IT Act") and the Information Technology Rules (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), 2011 ("SPDI Rules"), which have been India's data protection framework until now. The DPDPA is the first cross-sectoral law on personal data protection in India which is for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their data and the need to process such personal data for lawful purposes and matters connected therewith or incidental thereto.

Overview

The Act protects digital personal data (that is, the data by which a person may be identified) while recognizing the need to process such data. It does so by providing for the following:

- Defining the obligations of Data Fiduciaries (that is, persons, companies and government entities who process data) for data processing (that is, collection, storage or any other operation on personal data)
- Defining the rights and duties of Data Principals (that is, the person to whom the data relates)
- Imposing financial penalties for breach of rights, duties and obligations
- Establishment of the Data Protection Board of India

Scope of the Act:

The DPDPA is 'principles-based legislation' that relies on concepts that are broadly similar to those in the other legislations across the globe like GDPR. It governs data fiduciaries (i.e. data controllers), data processors and data principals (i.e. data subjects).

The DPDPA applies to the following:

- Personal data capable of identifying the data principal, which is either collected digitally or is digitized after it is collected nondigitally.
- Personal data processed for personal or domestic purposes or aggregated personal data collected for research and statistical purposes which is not used for any decision specific to a data principal are excluded from the DPDPA. Personal data made publicly available is also out of the scope of the DPDPA.
- Data that is processed within Indian territory or, if processed outside, is in connection with any activity relating to the offering of goods and services to individuals within India.

Highlights of the DPDPA:

- It applies to the processing of digital personal data within India where such data is collected online, or collected offline and is digitized. It also applies to such processing outside India if it is for offering goods or services in India. The Bill allows the transfer of personal data outside India, except to countries restricted by the central government through notification.
- Personal data may be processed only for a lawful purpose upon consent of an individual. Consent may not be required for specified legitimate uses such as the voluntary sharing of data by the individual or processing by the State for permits, licenses, benefits, and services.
- Data for minors (under the age of 18) is considered sensitive and requires clear and verifiable parent/legal guardian consent
- Right to Nominate, like a power of attorney, also applies where an individual may nominate other individuals to act on their behalf in case of death or incapacity.
- Data fiduciaries will be obligated to maintain the accuracy of data, keep data secure, and delete data once its purpose has been met.
- Organizations must appoint "Data Protection Officer(s)" – DPO's – and must be based in India
- It grants certain rights to individuals including the right to obtain information, seek correction and erasure, and grievance redressal.
- Government agencies are exempted from the application of provisions of the Bill in the interest of specified grounds such as security of the state, public order, and prevention of offenses.
- The central government will establish the Data Protection Board of India to adjudicate non-compliance with the provisions of the Bill.
- The Bill specifies penalties for various offenses such as up to:
  - (i) Rs 200 crore for non-fulfillment of obligations for children, and
  - (ii) Rs 250 crore for failure to take security measures to prevent data breaches.

Penalties will be imposed by the Board after conducting an inquiry

How can organizations Prepare themselves?

Organizations subject to the DPDPA have to address complex requirements such as processing of personal data, collecting and managing customer consent and Data Subject Rights requests (DSR's). Manual processing of these requirements poses a set of challenges, such as Labor costs and time delays, risk of human error, scalability issues, reputational risks and of course, Compliance risks!

Investing in a modern platform, experienced with other global data privacy regulations such as the GDPR and CCPA, and designed to manage and automate these workflows can significantly alleviate these challenges through:

- Streamlined Data Management
- Enhanced Security and Compliance
- Delegated User management for partners and third-party identities
- Empowering end-users
- Operational Efficiency through automation

How can Thales help:

Consent and Preference Management is an app exclusive to the Thales OneWelcome Identity Platform, dedicated to helping businesses and organizations comply with global data privacy regulations, and empowering users to maintain control over their data preferences. The identity app is centered around respecting individual data choices, enabling users to actively manage their consents and preferences, and exert influence over how their data is handled. It introduces the data privacy conversation explicitly with the end user as part of the user journey and interactions with a business or organization.

Implementing a modern Customer Identity and Access Management (CIAM) platform that includes Consent and Preference Management helps with "always-on" compliance with global data privacy regulations such the DPDPA, GDPR, CCPA/CPRA and more.

Consent and Preference Management benefits

Data Privacy conversation
Introduce the subject as part of the user journey by explicitly seeking end user consent

Empower End Users
Build and maintain trust with your end users by empowering them to control their data storage and processing preferences

Just-in-Time Consented Data
Collect consented data Just-in-Time to enable excellent user experiences

Compliance
Maintain compliance with not just the DPDPA, but an ever-growing list of global data privacy regulations

Key features

- Enables end-users to give and revoke consent
- Receive and manage fine-grained permission at the attribute level
- Facilitate multiple processing purposes on the same attributes
- Document consent with multi-lingual versioning
- Have a ''Single Source of Truth'' for consent and preferences
- Create a timeline with consented data
- Develop token enrichment with consent-related data
- Utilizing consent APIs for integrating consent in the full application landscape
- Have a central source for compliance reporting

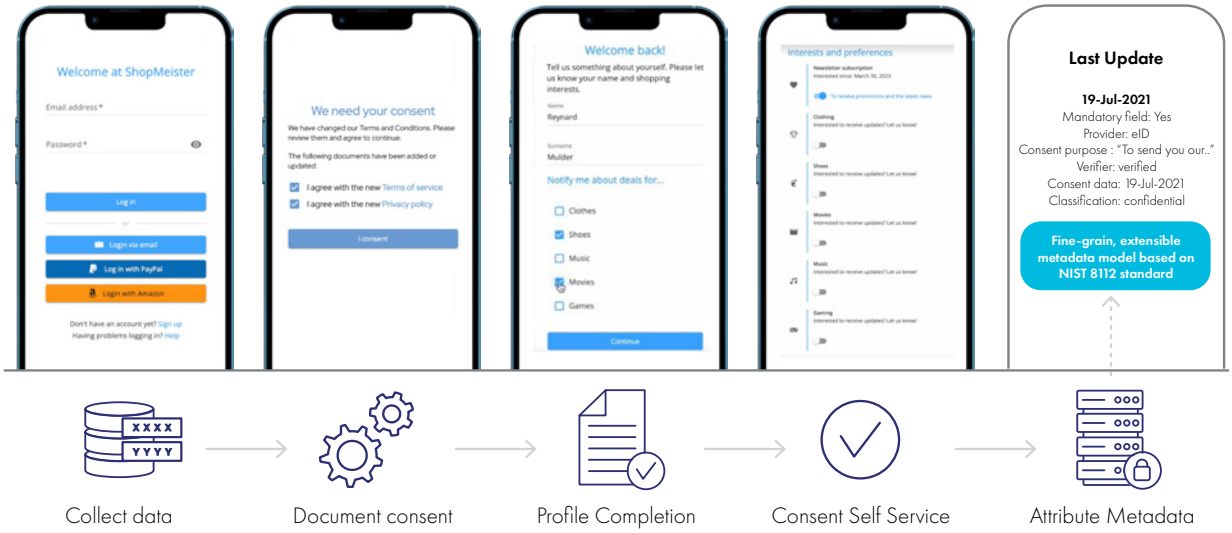
How does Consent and Preference Management work?

The Consent and Preference Identity App serves as a powerful tool for organizations to not only meet regulatory requirements but also to build more trustworthy relationships by prioritizing transparency, user empowerment, and compliance. By seamlessly integrating consent mechanisms into the identity lifecycle processes, the Consent and Preference management identity app ensures that the data conversation is brought to the forefront of the user's experience. Through intuitive self-service features, users gain the ability to manage their consent and preference settings with ease.

The Consent and Preference Management identity app manages end user's consent and attribute preferences (i.e., current consent, tracking consent on policies and attributes, tracking consent on user data etc.), while processing their data in a compliant and secure way. As a result, businesses can focus on securely connecting consumers with their online services and apps, protecting their data, and analyzing identity behavior for better engaging customer experiences.

Thales OneWelcome allows clients to support the entire consent lifecycle, giving end users a single view and control over all their consents, and assisting them in exercising their consumer rights regarding data privacy: the right to view, export and edit all their personal data stored within Thales OneWelcome Identity Platform at any time, as well as the right to request to freeze their accounts and delete their personal data.

Make privacy and consent an integral part of your user journey



Capturing end-user's Consent & Preference settings

An important success factor for businesses looking to inject simplicity and build trust in their identity registration process lies in establishing a data privacy conversation with their end users. The key is to effectively gather:

- End user's consent for (updated) documents like privacy statements and terms of service
- Preferences and consents for all data attributes besides the ones they need for your services to operate in a compliant fashion
- All processing purposes related to these consent and preference settings

Additionally, end-user's should be able to withdraw consent at any time, just as easily as they gave it. This helps businesses realize that consent is not a ''once given'' but has a lifecycle through which it builds trusted relationships.

Why leading companies trust Thales

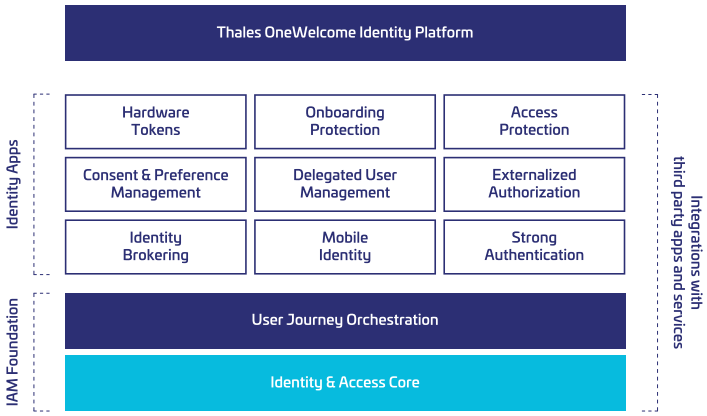
Leading companies around the word rely on Consent and Preference Management capabilities from Thales. Our cloud-based identity platform is an agile, future-proof solution built upon best practices and the industry's strictest standards for security and performance.

Gain customer loyalty by building – and maintaining – customer trust through Consent and Preference Management

Create high-quality Customer profiles in a compliant manner
Always-on compliance enables companies to build rich, unique customer profiles.

Increase sign-ups and registration
With Just-in-Time consented data, coupled with progressive profiling, streamline and simplify your customer registration process. Only ask for necessary information needed to perform a particular action.

Establish and build trust through transparent consent processes
Allow customers to add, change or remove consent at key moments of the customer journey, essentially giving end-users better control of their own data



About Thales

Thales is a global leader in data security, trusted by governments and the most recognized companies around the world to help them protect their most sensitive data. The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

cpl.thalesgroup.com

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us