IKIGAI LAW

Complying with India's DPDP Act and Rules

Impact and roadmap for Japanese Businesses

Note: *This presentation is for discussion purposes only and does not include advice on any specific issues.*

About Us:

IKIGAI LAW

Who we are?

Award winning law and policy firm, with a sharp focus on technology and innovation.

What do we do?

360º approach: law, policy and GR. Sectoral expertise in data, e-commerce, fintech, cloud, cybersecurity, emerging technologies, intermediary liability, among others.

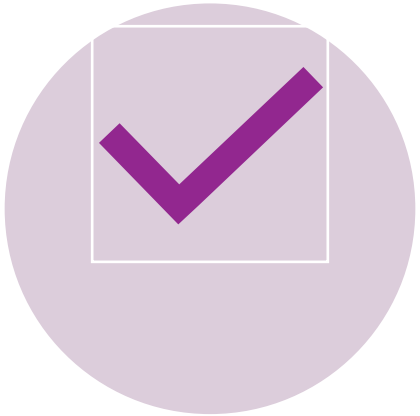
Who do we work with?

Technology companies, start-ups, governments, VCs, industry bodies, and think tanks.

Overview

IKIGAI LAW

PROJECT PLAN FOR COMPLIANCE



IMPLEMENTATION GUIDANCE FOR KEY OBLIGATIONS

ROAD AHEAD / WHAT IS NEXT

Status and timelines - DPDP Act and Rules

IKIGAI LAW

- On 14 November 2025, the Indian government notified the DPDP Rules, bringing the DPDP Act into force.
- Data Protection Board related provisions take effect immediately i.e. 14th November 2025.
- Obligations related to consent managers come into force 1 year from publication i.e. 14th November 2026.
- All substantive obligations (notice, consent, breach reporting etc.) come into force 18 months from publication i.e. 14th November 2027

Project plan for DPDP compliance

STAGE 1: Data Discovery and Inventorization

IKIGAI LAW

- **Objective**: To gain visibility into data handling practices across teams.
- **Document**: Data record sheet/questionnaire filled by each team to map their data handling practices.
- **Timeline**: 1-2 months

STAGE 2: Gap Assessment / Readiness Assessment

IKIGAI LAW

- **Objective**: To conduct a gap assessment on how the organization as a whole and each team's data handling practices fare when compared with the DPDP Act and DPDP Rules and assess next steps. This will consist a review of:
  - **Front End Assessment (B2C):** User facing processes such as providing privacy notice/policies, obtaining user consent, providing mechanism for user rights and overall UI/UX.
  - **Back End Assessment (Internal):** Back-end processes such as, creating a data inventory, implementing a breach reporting mechanism, creating SOPs for data deletion.
  - **Contractual (B2B):** Contracts with vendors, service providers, partners, employees; ascertain how you (i) share data with third-parties; and (ii) receive data from third-parties. Re-negotiate contracts to cap your liabilities.

STAGE 2: Gap Assessment / Readiness Assessment (Cont.)

IKIGAI LAW

- **Documents**:
  - Gap assessment report mapping the requirements under the law, the organizations' current data practices and gaps in compliance.
  - Roadmap/compliance document for next steps/action items to bridge the gap and comply with the law.
  - Data Protection Addendums/ clauses added in contracts.
- **Timeline**: 2-3 months

STAGE 3: Drafting documents/ policies

IKIGAI LAW

- **Objective**: Have in place internal and external documents required to comply with the DPDP Act and DPDP Rules.

- **Document**:
  - *Website privacy policy/privacy notice*
  - *Cookie notice*
  - *Policy for data retention and disposal*
  - *Policy for responding to user requests for data*
  - *Breach/ incident response policy*
  - *Employee privacy notice*
  - *Employee handbook*

- **Timeline**: 2 months

Implementation guidance for key obligations

Notice and Consent

IKIGAI LAW

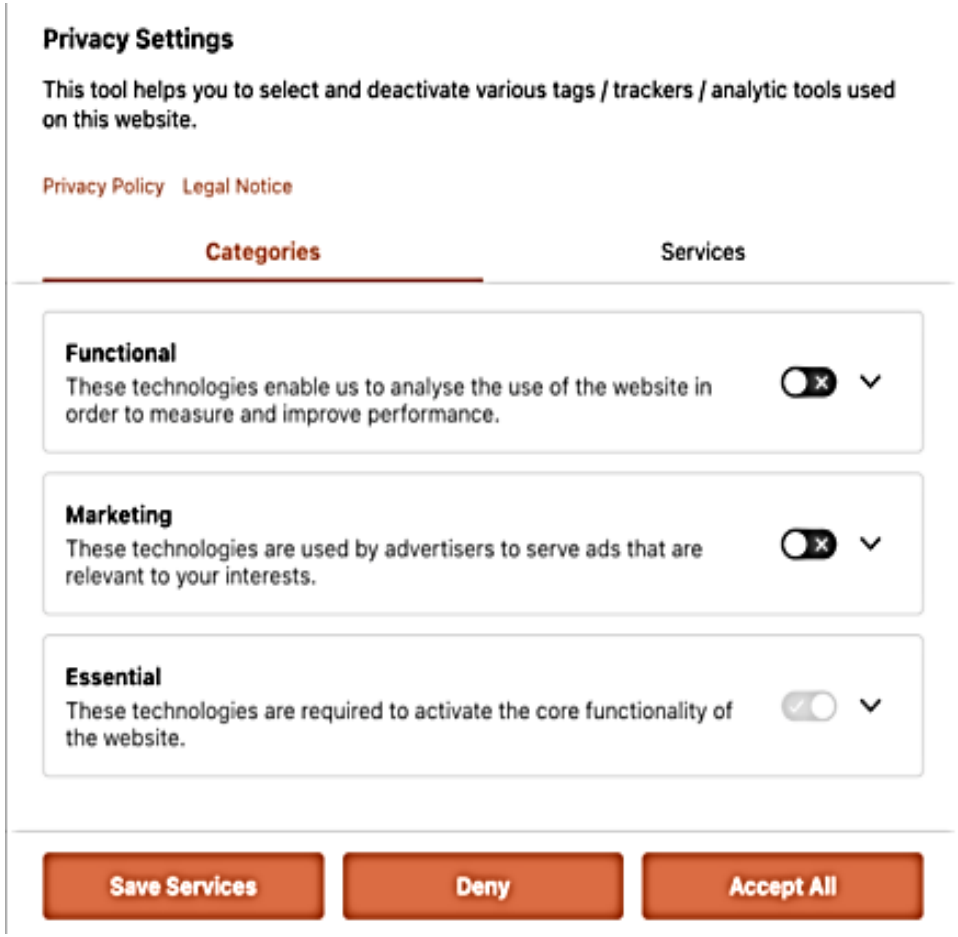
Requirements

- Presented in clear and plain language.
- Understandable “independently” of other information given to users.
- Should contain a “fair account of details” to allow users to give informed consent.
- Itemised list of personal data linked with specified purpose and specific description of goods/services or uses.
- Link to website/ app to allow users to withdraw consent, exercise rights, complain to the Data Protection Board.

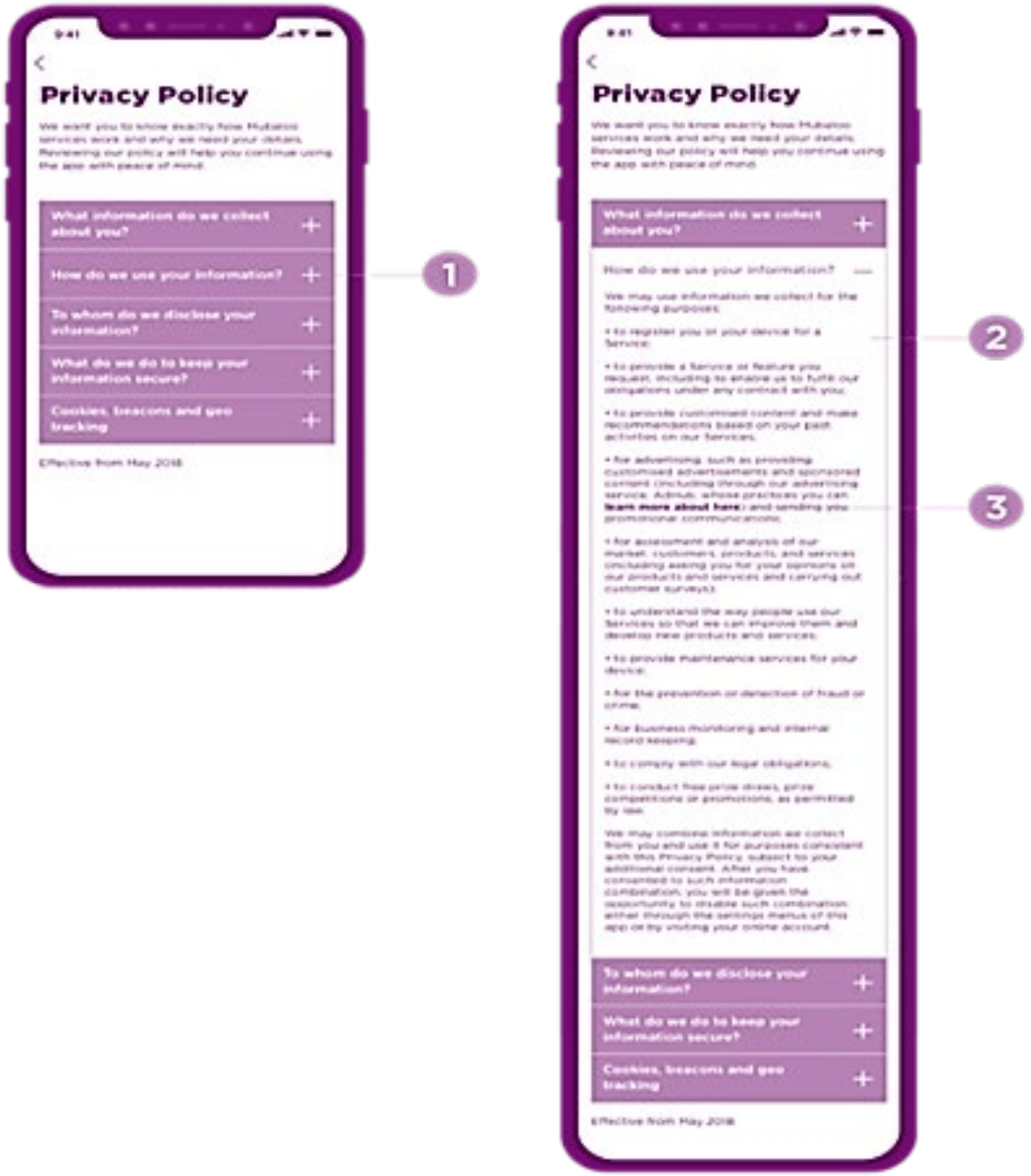
What should you do?

- Merely linking the privacy policy and terms of use will not suffice. Provide a more detailed notice during sign-up.
- Update privacy policies. Prepare laundry list of data processed and map it to specific purposes.
- Review your UI/UX to provide notices on the UI itself. Explore smart design through layered notices, intermediate screens, drop-downs.

Notice and Consent



Consent through pop-up(s)



Layered Privacy Policy

Notice and Consent

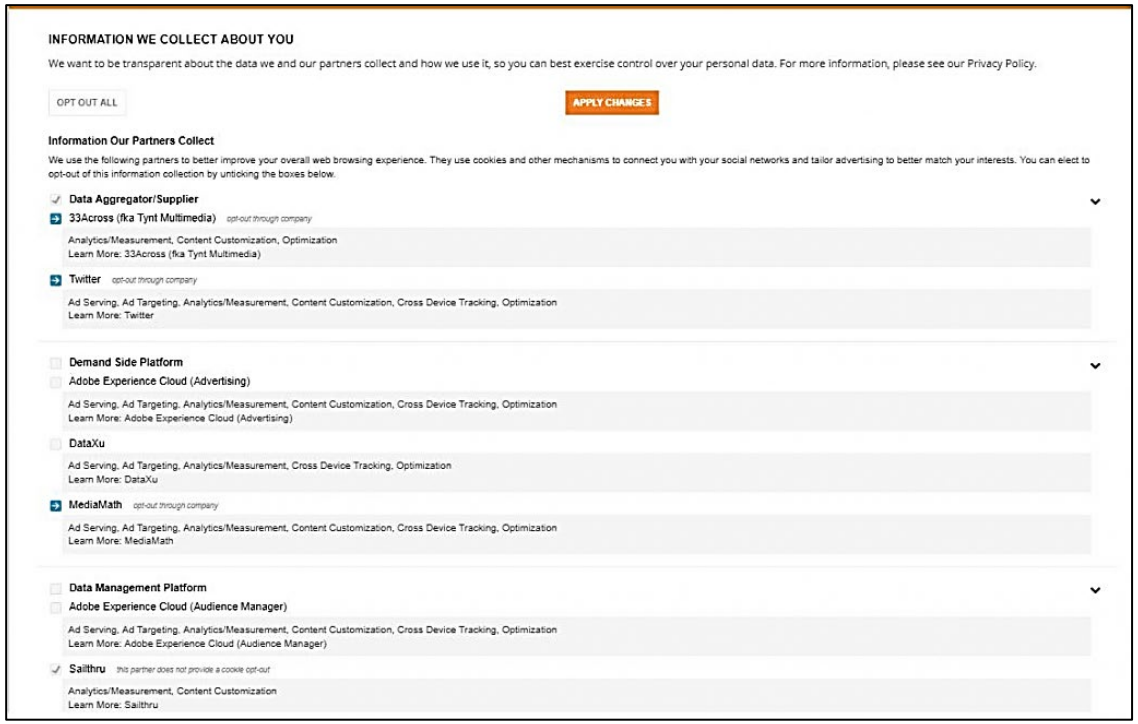
What may not work:

By signing up, I agree to terms

+91 Enter your mobile number

Continue

Catch-all consent with hyperlinks



INFORMATION WE COLLECT ABOUT YOU

We want to be transparent about the data we and our partners collect and how we use it, so you can best exercise control over your personal data. For more information, please see our Privacy Policy.

OPT OUT ALL

APPLY CHANGES

Information Our Partners Collect

We use the following partners to better improve your overall web browsing experience. They use cookies and other mechanisms to connect you with your social networks and tailor advertising to better match your interests. You can elect to opt-out of this information collection by unticking the boxes below.

Data Aggregator/Supplier

33Across (fka Tynt Multimedia) opt-out through company

Analytics/Measurement, Content Customization, Optimization
Learn More: 33Across (fka Tynt Multimedia)

Twitter opt-out through company

Ad Serving, Ad Targeting, Analytics/Measurement, Content Customization, Cross Device Tracking, Optimization
Learn More: Twitter

Demand Side Platform

Adobe Experience Cloud (Advertising)

Ad Serving, Ad Targeting, Analytics/Measurement, Content Customization, Cross Device Tracking, Optimization
Learn More: Adobe Experience Cloud (Advertising)

DataXu

Ad Serving, Ad Targeting, Analytics/Measurement, Cross Device Tracking, Optimization
Learn More: DataXu

MediaMath opt-out through company

Ad Serving, Ad Targeting, Analytics/Measurement, Content Customization, Cross Device Tracking, Optimization
Learn More: MediaMath

Data Management Platform

Adobe Experience Cloud (Audience Manager)

Ad Serving, Ad Targeting, Analytics/Measurement, Content Customization, Cross Device Tracking, Optimization
Learn More: Adobe Experience Cloud (Audience Manager)

Sailthru this partner does not provide a cookie opt-out

Analytics/Measurement, Content Customization
Learn More: Sailthru

Pre-checked consent boxes

Data retention and deletion

IKIGAI LAW

Requirements

- Delete data when purpose for collection is served. Flexibility in determining timelines.
- For specific businesses (e-commerce platforms and social media intermediaries with 2 crore users, online gaming intermediaries with 50 lakh users) – delete personal data of inactive users after 3 years of inactivity.
- Businesses must retain personal data, traffic data, and processing logs for at least 1 year, for purposes of national security, legal purposes, or assessment of SDFs. After 1 year, the data must be deleted unless another law requires longer retention.
- **Inactivity**: User does not: log into their account, initiate contact, exercise their rights. 3-year countdown from when rules take effect or last user interaction, whichever is later.
- Notify such users 48 hours before deletion.
- **Exceptions**: Data required for legal compliance (tax, accounting, etc.), data required to enable user to access her account and access tokens/ get accrued benefits.

What should you do?

- Establish deletion protocols, including internal flags when accounts remain dormant.
- Notify users (in-app/email/SMS) 48 hours before deletion.
- Evaluate retention timelines for each record that you maintain under different applicable laws.
- Establish systems to retain personal data for 1 year
- Implement periodic review of records. Sensitize employees on retention/ deletion requirements.

Breach reporting

IKIGAI LAW

Requirements

- In case of a data breach, report immediately to:
    - Affected individuals with details of the breach, potential consequences, and mitigation measures, mitigative measures she can take, contact information of person who will answer queries of individuals on behalf of DF
    - Data Protection Board (**Board**) with description of the breach, its nature, extent, timing, location and likely impact.
- Detailed reporting to the Board within 72 hours, covering the facts of the breach, remedial and mitigation measures, details of persons responsible for breach.

Breach reporting

IKIGAI LAW

What should you do?

- Recalibrate incident response protocols to align with the regulatory requirements.
- Internal training among different teams to identify and report breaches.
- Internal workflows to meet:
  - Reporting requirements to the Board.
  - Reporting mandates of the Computer Emergency Response Team India (CERT-In).
  - Sector-specific regulatory requirements, where applicable.
- Ensure timely communication to affected individuals.
- Establish templates/SOPs for different scenarios.
- Protocols to foster seamless coordination among legal, technical, and communications teams.

Enabling User Rights

IKIGAI LAW

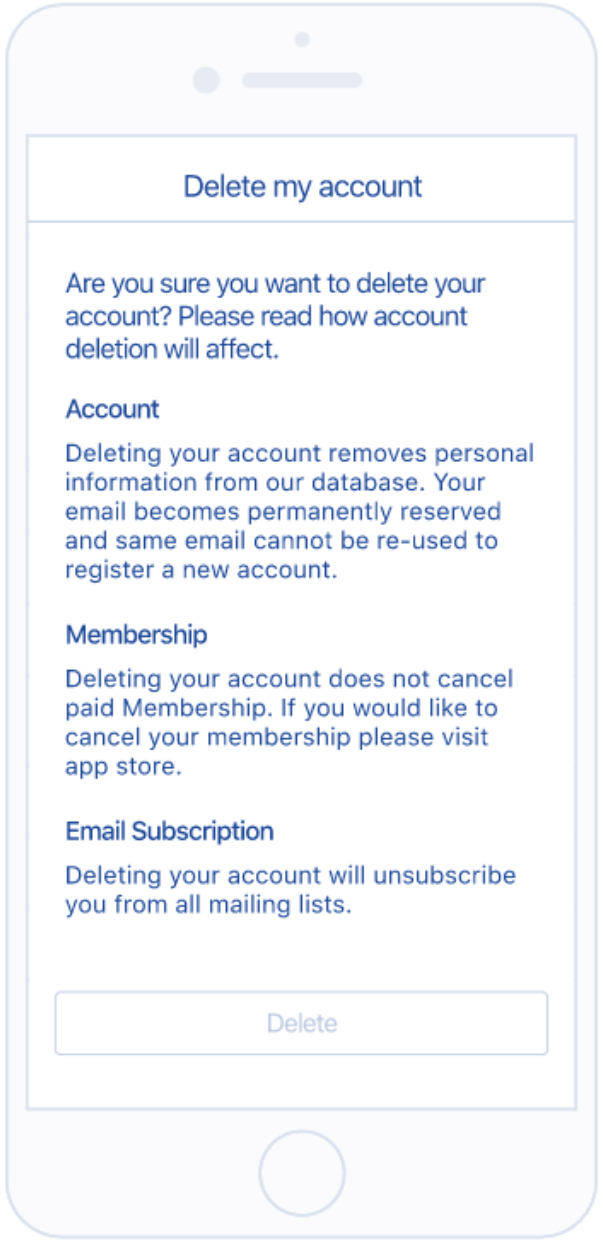
Requirements

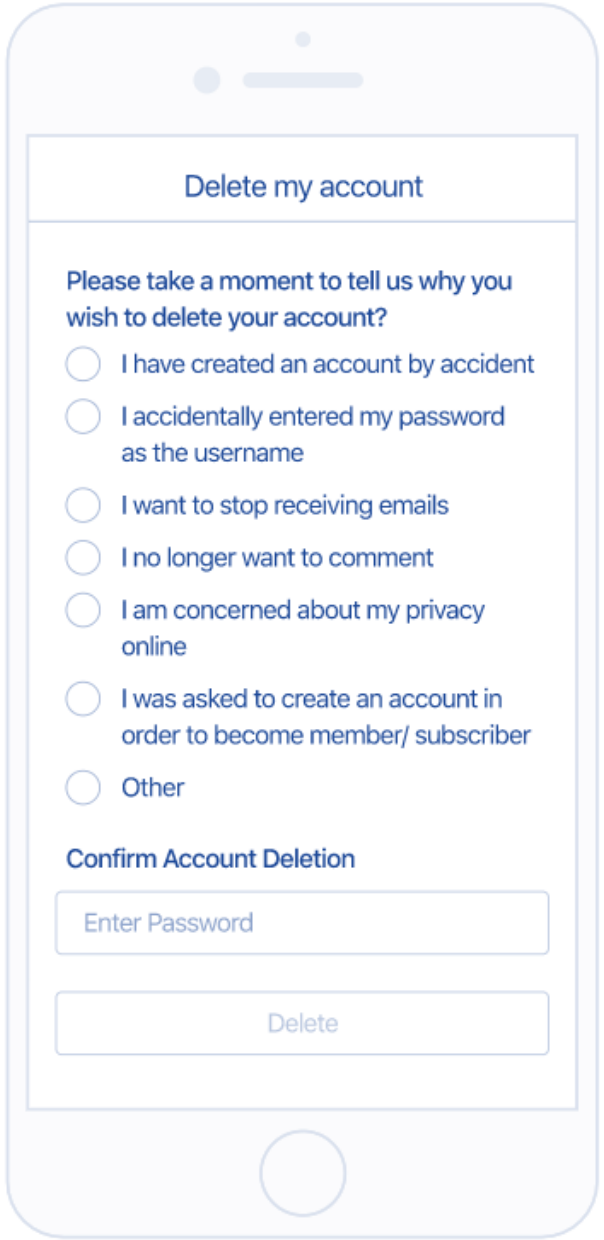
- Publish clear and easily accessible methods for users to request data access and erasure.
- Implement mechanisms for users to easily exercise their rights under the DPDP Rules.

What should you do?

- Automate user rights processes, such as data access requests and data deletion requests.
- Develop clear communication channels, such as dedicated support portals or helplines, for user queries related to data privacy.
- For e.g. Provide user-friendly dashboards on platforms that allow users to easily access, modify, and delete their personal data.

Example:
User rights.





IKIGAI LAW

Grievance redressal mechanism

IKIGAI LAW

Requirements

- Display business contact details of grievance officer on platforms.
- Publish response timelines (not exceeding 90 days) for user grievances.

What should you do?

- Robust processes for grievance redressal.
- Establish timelines for responses/ redressal.
- Enable automated options, such as self-service menu to the extent possible.

Reasonable security safeguards

IKIGAI LAW

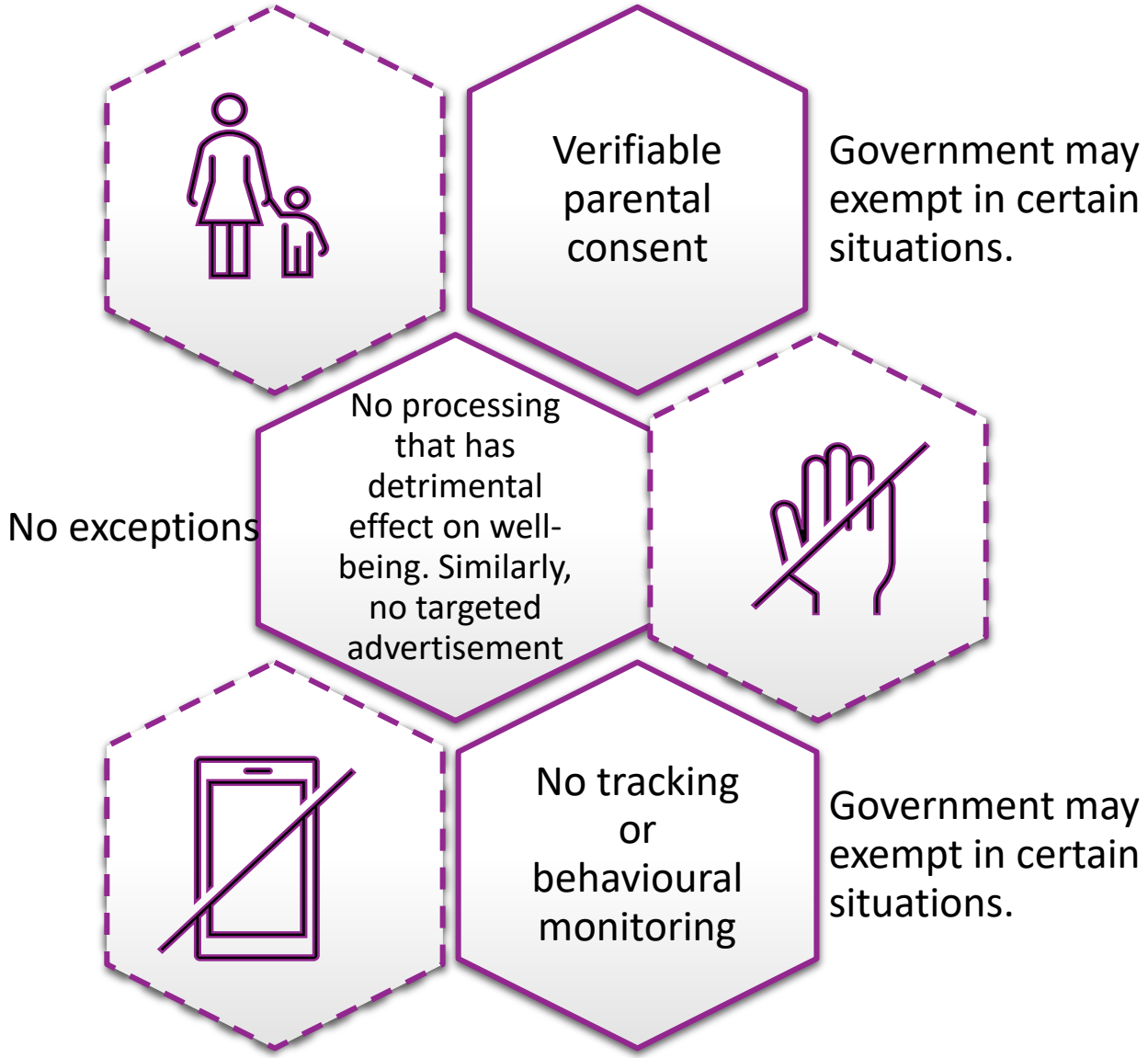
Requirements

- Businesses must implement reasonable security safeguards, including:
  - Encryption, obfuscation, masking, and virtual token mapping.
  - Strict access controls to computer resources.
  - Monitoring and logging for detecting unauthorized access.
  - Data backups for continued processing in case of data compromise.
  - Retaining logs for at least one year.
  - Including security requirements in contracts with data processors.

What should you do?

- Review and update existing security measures to meet the baselines in the rules.
- Align with international standards like ISO 27001, which broadly track with DPDP.
- Update contracts with data processors to incorporate required safeguards.

Processing Children's data



Age:

Children < 18 years

But if processing activities are in a “verifiably safe” manner, then a lower age may be prescribed.

Processing Children's data

IKIGAI LAW

Requirements

- Ensure appropriate organisational and technical measures to get parents' verifiable consent before you process children's data. Child is any user <18 years of age.
- Conduct "Due diligence" to verify person giving consent is an adult.
- If parent is an existing user of the platform – use "reliable details" of age and identity available with the fiduciary. If parent is a new user – use voluntarily provided details of age and identity/ tokens issued by government-authorised entities.
- Prohibition on tracking, monitoring and targeted ads. Exemptions for certain purposes (preventing harmful content, location tracking etc).

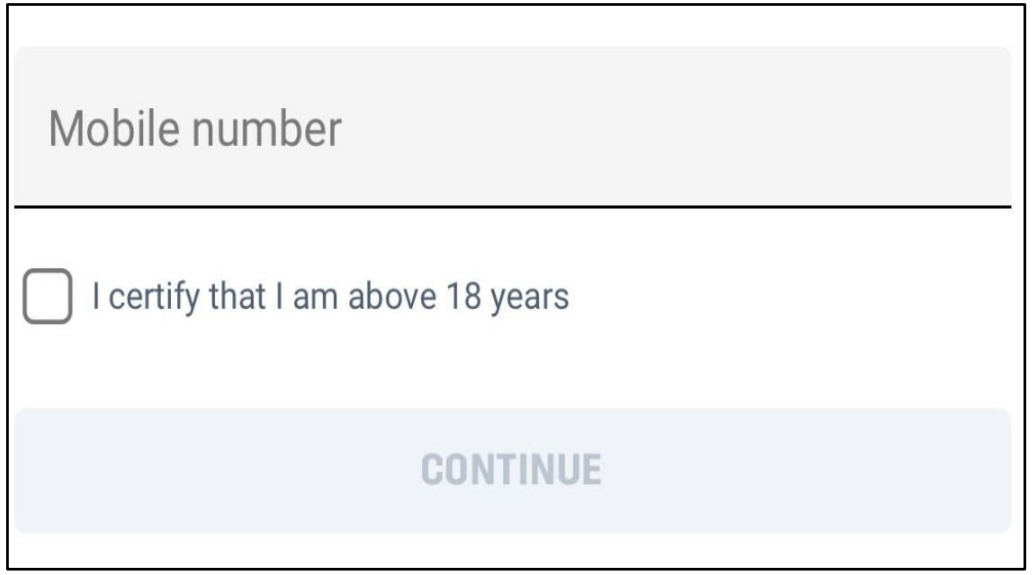
What should you do?

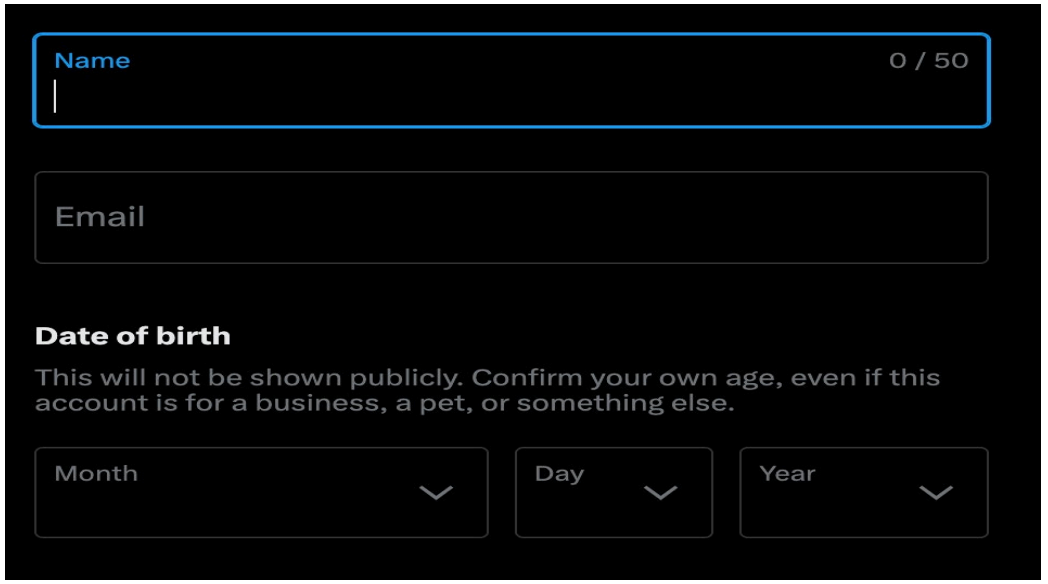
- Unclear whether this means age-gating the Internet. A more pragmatic view would be that only platforms that are directed at children or know that they are dealing with a child must age gate.
- Evaluate type of age-gate – a self-declaration, neutral age-gate, age token through third parties, other sophisticated means.
- Evaluate means of parental consent – credit card on file, behavioural data, government IDs.
- Evaluate whether any of the exceptions apply. If not, re-engineer to ensure that you do not track or monitor children or show them targeted ads.

Processing Children's data

IKIGAI LAW

Examples of Age-gates





Cross-Border Data Transfers

IKIGAI LAW

Requirements

- Data Fiduciaries – Transfer is allowed, subject to businesses meeting conditions prescribed by the Central Government for sharing data with foreign governments or entities.
- Significant Data Fiduciaries (SDFs) – Transfer of some category of data will be restricted. Notification of such category will be recommended by a government-formed committee

What should you do?

- Ensure compliance with government conditions for all cross-border data transfers.
- Prepare for potential localization requirements if designated as an SDF.

Additional measures for Significant Data Fiduciaries (SDF)

IKIGAI LAW

Requirements

- Conduct annual Data Protection Impact Assessments (**DPIAs**) and audits (possibly independent third-party audits).
- Submit findings of DPIAs and audits to the Board.
- Verify technical measures like algorithmic software for potential risks to data principals' rights.
- Adhere to potential restrictions on cross-border transfers of personal and traffic data.

What should you do?

- Business processing sensitive data, e.g. financial details, health data, or voluminous data may consider preparing for potential classification as an SDF (***for now,*** no further guidance on who will be SDFs)**.**
- Align the use of Artificial Intelligence (AI) and Machine Learning (ML) in business to identify and gauge any possible violation of users' rights.

Handling Government Requests

IKIGAI LAW

Requirements

- Government can request information for national security, legal compliance, assess SDF designation.

What should you do?

- Establish robust internal systems for handling requests.
- Ensure readiness for quick turnaround times.

The Data Protection Board

Composition

- Board to consist of Chairperson and other Members, appointed by the Central government–in total 4 members. Head office in Delhi NCR.
- Search-cum Selection Committee to be formed for selection of **Chairperson** of the Board.
    - Search-cum Selection Committee to comprise of (a) Cabinet Secretary, (b) Secretary – Ministry of Electronics & IT, (c) Secretary–Department of Legal Affairs and (d) two experts of repute (having special knowledge or practical experience in a field which may be useful to the Board.
- Search-cum Selection Committee for selection of **Members** to comprise of (a) Secretary – Ministry of Electronics & IT, (b) Secretary– Department of Legal Affairs and (c) two experts of repute.

Qualification

- Board Chairperson and Members to be individuals of ability, integrity and standing.
- Having special knowledge or practical experience in the fields of: Data governance, administration or implementation of consumer protection and social laws, dispute resolution, Information and communication technology, digital economy, law, regulation or techno-regulation, or any other filed useful for the Board (in the opinion of Central government).
- At least one Member of the Board should be an expert in the field of law.

Powers of the Board

- Can direct urgent remedial or mitigation measures in case of a breach.
- May inquire into breaches and impose penalties as specified in the DPDP Act.
- Inquires into complaints from Data Principals about personal data breaches or breaches by Data Fiduciaries or Consent Managers.
- Can also inquire into breaches related to the registration of Consent Managers.
- Can inquire into breaches referred by the Central Government regarding intermediaries' obligations.
- After hearing the concerned person, the Board can issue binding directions for remedial action.

Functioning of the Board

- The Board will function as a digital office which may adopt techno-legal measures to conduct the proceedings in a manner which does not need physical presence of any individuals.

Penalties:

IKIGAI LAW

Subject Matter	Amount
Failure to undertake reasonable security safeguards.	Rs 250 crores
Failure to provide breach notification.	Rs 200 crores
Children Data - failure to comply with additional obligations.	Rs 200 crores
Significant Data Fiduciary - failure to comply with additional obligations.	Rs 150 crores
Breach of other provisions.	Rs 50 crores

Appeals

IKIGAI LAW

- Any person aggrieved by an order or direction of the Board may file an appeal before the Appellate Tribunal (Telecom Disputes Settlement and Appellate Tribunal).
- Appeal must be filed within 60 days from the receipt of the Board's order, unless sufficient cause is shown for the delay.
- The Appellate Tribunal may confirm, modify, or set aside the order after giving parties an opportunity to be heard.
- Appeals must be disposed of within 6 months, and if not, reasons must be recorded.
- Appeals, including related documents, must be filed digitally. Fees for appeals align with those under the Telecom Regulatory Authority of India Act, 1997.
- The Appellate Tribunal functions as a digital office, adopting techno-legal measures to conduct proceedings without requiring physical presence.
- The Appellate Tribunal is not bound by the Code of Civil Procedure but follows the principles of natural justice and regulates its own procedure.

Alternative Dispute Resolution and Voluntary undertaking

IKIGAI LAW

Alternative dispute resolution

- The Board may direct the resolution of any complaint through mediation, if it feels that the complaint can be resolved through mediation.

Voluntary undertaking

- Board can accept a voluntary undertaking from any person at any stage of proceedings.
- The undertaking may include – (a) Actions to be taken or actions to refrain from, within a time frame determined by the Board, and (b) Publicizing the undertaking if deemed necessary by the Board.
- The Board can, with the consent of the person who gave the undertaking, modify the terms of the voluntary undertaking.
- Once accepted, the voluntary undertaking bars further proceedings under the Act on matters related to the undertaking, unless the person fails to comply with the terms.
- If the person fails to comply with the terms of the voluntary undertaking, it constitutes a breach of the Act.
- The Board may proceed with actions, after giving the person an opportunity to be heard.

IKIGAI LAW

Thank you

Contact us:

pallavi@ikigailaw.com
sreenidhi@ikigailaw.com