BUSINESS GUIDE: COMPETITIVE AND EASY DATA PROTECTION

POOVAYYA
ADVOCATES & SOLICITORS

India's Digital Personal Data Protection Act, 2023 (DPDP Act), is expected to come into force soon. The Government has advised businesses to comply with the Act although it is yet to be notified. Learn more in our article here.

Meanwhile, other regulators are already active in the consumer protection space, with the Competition Commission of India imposing a nearly USD 25.4 million fine on Meta for its unilateral amendments to its privacy policy in 2021.

In the EU, regulations are tightening further on the use of tracking technologies such as tags, pixels (and of course) cookies.

In the US as well, the FTC is carrying out several measures, auditing businesses for their practices around data collection and consumer rights.

Businesses need a way to ***further their goals and achieve results*** - customer acquisition, reduced churn, increased revenue and so on - while ***respecting customer privacy and data protection regulations***. In fact, trust and respect for customer rights is becoming a competitive advantage that businesses can leverage - if they can take the correct steps.

Do you have the strategy and tools to achieve this?

Here are some ***actionable takeaways*** for businesses to align their data-related activities with compliance requirements.

Data Collection Points: The DPDP Act sets out requirements to collect and process data tied to specific purposes. This means considering, at the point of collection, why data is being collected, and how it will be used. **Remember** - this includes both active data collection (where the customer provides data) and passive data collection (data collection without the customer's active involvement, such as device data, location data, etc.).

Takeaway No.1: Consider all the data items collected, and what they will be used for. Ensure there is a specific justification for each data item that is collected and processed. Collecting data without a clear, specific purpose is not recommended.

Data Processing Purposes: Once collected, how is the data used? Is it used for one or multiple purposes? It is crucial to determine the purpose/purposes for each data item.

Takeaway No.2: Map each data item to all the purposes for which it is used.

Basis for Processing: Each processing activity needs a lawful basis, as specified under the DPDP Act. Consent is the primary lawful basis, but others may apply depending on the context.

Takeaway No.3: Map each processing activity to a lawful basis. If any activity lacks a lawful basis, you are exposed to (potentially significant) liability.

Data Retention and Security: Assess data storage, retention and security. Ensure secure data storage and handling (including during data transit). Evaluate internal policies related to data retention to determine if they are appropriate for each data item.

Takeaway No.4: How does your business store data? What information security measures has your business implemented? How long do you store each data item? Exact timelines don't always need to be specified, but a considered approach is necessary.

Data Sharing: Data sharing, even among affiliated entities, is under increasing scrutiny. The CCI's ruling against Meta highlights the risks involved when data is shared without explicit consent.

Takeaway No.5: Is customer data shared with group entities or external parties? Are customers informed, and have they consented? If not, check if other lawful bases, like voluntary data provision, may apply.

Transparency to Customers: Ensure that customers are adequately informed about data collection/usage, sharing practices, etc. Transparency is particularly important when seeking customer consent for data processing.

Takeaway No.6: Do you have a transparent privacy policy and consent flow? Does it address all relevant aspects of data handling?

Final Takeaways for Business: Review your data practices and be ready to answer these questions:

1. **What customer data is collected?**
2. **Why is this data collected?**
3. **How is the data used?**
4. **How is the data stored and secured?**

5. **Is the data shared with any other entities (affiliates or third parties)?**
6. **Are customers informed about all these aspects?**

Data protection doesn't have to be daunting. Usually, what's required is simply:

- ☑ A clear understanding of the data practices of your business;
- ☑ Adopting a risk-based approach to assess those data practices; and
- ☑ Implementing commonsense measures to ensure compliance.

The challenge lies in integrating these measures into your business operations while balancing practical needs. This is where expert guidance can make a significant difference in transforming compliance from a burden to a strategic advantage.

Our Data Protection/AI practice specialises in helping businesses navigate these complex requirements efficiently and effectively. Reach out to us if you'd like to know more.

Get in touch:

Siddhartha George
Practice Head, Corporate
siddhartha@poovayya.net

Harini Sudersan
Partner, Data Protection/AI
harini@poovayya.net

POOVAYYA
ADVOCATES & SOLICITORS