How Evolving Data Privacy Laws Are Shaping The Indian Startup Ecosystem

Evolving data privacy laws are impacting businesses globally and locally, with startups facing increased accountability in managing sensitive data

Compliance requirements and costs have risen, forcing startups to invest in achieving compliance and avoiding penalties

Startups must also adapt their business processes and systems to meet new data privacy laws, which may require technology investments, staff training and process redesign

Data protection is challenging for many businesses, especially those operating in multiple countries facing challenges with growing data privacy regulations. Since 2018, the year the European Union's General Data Protection Regulation (GDPR) came into effect, it has had a domino effect, and data privacy laws have indeed started expanding in many jurisdictions around the world.

Many countries are adopting data privacy laws inspired by the GDPR. For example, in 2020, Brazil enacted the General Data Protection Law (LGPD), which established regulations for personal data processing and granted rights to individuals akin to those in the GDPR. This was similar to the California Consumer Privacy Act (CCPA) in the United States.

South Korea and Thailand, among other Asian countries, have updated their data protection laws to reflect this global trend of enhancing data privacy regulations. These developments demonstrate a collective effort to safeguard personal information and empower individuals with greater control over their data.

The evolving laws are having an undeniable impact on businesses both locally and globally. Gartner anticipated 65% of the world's population would have its data covered under modern privacy regulations by 2023. Thus, businesses operating globally are now compelled to adapt to a wide range of regulations, often with different requirements and restrictions.

How Evolving Data Policies Impact Startups

The expansion of data privacy laws has had a significant impact on startups. Here are some ways in which these laws affect them:

Compliance Requirement & Cost

The widespread implementation of data privacy regulations across the globe also increases specific compliance obligations that startups must adhere to. Such implementations may vary from obtaining explicit consent from individuals to collect and process their data to implementing appropriate security measures to protect data, provide access to data and more.

The compliance requirement is directly proportional to cost because startups need more resources to keep up with evolving data regulations. Startups are compelled to invest in achieving compliance considering the substantial penalties associated with non-compliance and the potential risk of damaging their brand value.

Increased Accountability

The evolving data privacy laws have significantly increased the accountability of startup businesses when managing sensitive data.

Businesses must maintain comprehensive records of their data processing activities to ensure safe storage and analysis, identify risks involved in the data processing and conduct data protection impact assessments for high-risk processing, among other activities.

Impact On Business Processes

Adopting new data privacy laws may require startups to review and modify their internal processes and systems.

This could involve updating privacy policies, implementing more robust security measures, conducting privacy impact assessments for new projects, ensuring data minimisation and purpose limitation, and establishing mechanisms for data subject rights requests. These changes may require investments in technology, staff training, and process redesign.

Customer Expectations & Trust

With increased awareness about the importance of the protection of personal data and misuse of the same in recent incidents, data privacy has become a significant concern for individuals.

Customers expect startups of all stages and sizes to ensure and prioritise their personally identifiable information (PII) security. Adhering to recent and geographically suitable data privacy laws helps startups maintain a positive reputation and build stronger customer relationships.

Methods To Comply With Data Privacy Laws

Identify, Classify & Locate Sensitive Data

For any business, it is crucial to check where the data that is subject to specific protection requirements resides within the systems.

This understanding helps accurately identify the data lifecycle and its associated security risks. Enterprises conduct data mapping exercises to understand the flow of data within the system.

Safe Backup

Safe backup is crucial for effective data privacy governance as it helps maintain secure data backups in place. It provides organisations with a reliable and recoverable copy of lost or compromised data in the event of data breaches, system failures, or other incidents.

It also protects against ransomware attacks and mitigates the impact of the attack.

Data Encryption

Securing sensitive information across various business processes ensures that the business data is safe from outsiders. Data encryption ensures that sensitive data is converted into an unreadable format using cryptographic algorithms and only be accessed and understood by authorised teams or individuals. This prevents unauthorised individuals, including hackers or malicious insiders, from accessing and understanding sensitive data.

Encryption of data should happen at rest (when it is stored in databases, servers, or other storage systems) as well as in transit (when data is transmitted over networks or between systems) example, encryption protocol like Transport Layer Security (TLS) is used. Encryption facilitates secure data sharing and collaboration between authorised parties.

Employee Training & Awareness

Provide regular training and awareness programmes to employees about data privacy and security. Educate them on the importance of data protection, the handling of personal data, and the potential risks associated with non-compliance.

Phishing is one of the biggest threats to any business data security, and educating employees about phishing and raising awareness about its risks is crucial for businesses to mitigate this threat effectively.

Automation With Data Privacy Management Tools

Leverage data privacy management tools to streamline compliance efforts. Privacy tools can help startups and businesses maintain data privacy in several ways. The tools provide robust data governance capabilities, enabling enterprises to define and enforce privacy policies and access controls.

It ensures that personal information is accessed only by authorised individuals and used within the boundaries of consent. Thus, the usage of tools like this help to incentivise the steps taken towards protecting and securing data into a competitive advantage.

For example, a data fabric and micro-database solution can help preserve the data privacy of users and customers with the help of various data masking functions. Data masking provides the means to protect sensitive data while retaining its usability. It also employs several data masking techniques, including data scrambling, data blinding and data shuffling, to ensure the privacy of sensitive data. This approach involves ingesting, organising, processing and delivering data based on business entities such as customers, orders or devices.

This entity-based data masking supports both dynamic data masking for operational use cases like customer 360 and static data masking for test data management and legacy application modernisation. One such data masking solution I have used is called K2view. It addresses this challenge of locating sensitive information, including unstructured data (images, PDFs, text files and more), by incorporating an auto-discovery mechanism that scans data sources, classifies PII/PHI and applies masking techniques based on pre-defined rules.

Such an automated process allows for the efficient identification and mapping of sensitive data through an integrated data catalogue. The solution anonymises data across various sources like relational databases and non-relational databases like NoSQL.

Conclusion

Data privacy standards and regulations enable businesses to optimise their data management practices and help shape modern business practices transactions. By adhering to these regulations and implementing robust data privacy strategies, businesses can optimise their operations while safeguarding the privacy of their customer’s data.