**Data Privacy in India**

The Indian government may pass a Personal Data Protection Bill to restrict the collection, processing, storage, use, transfer, protection, and disclosure of Indian residents' personal data. DPB is significant for global managers while being regional. India's digital economy might be worth $1 trillion by 2022, attracting foreign businesses who must comply with DPB. India has followed the EU's GDPR in allowing global digital corporations to conduct business under specific restrictions, instead of China's isolationist framework that forbids global players like Facebook and Google from functioning within its borders. Indian DPB has more clauses than EU law. Because India is a nation state, it would consider citizen data as a national asset, retain and defend it inside national limits, and utilise it to protect its security and strategic interests. The DPB requires corporations to adapt their business models, methods, and beliefs. Others increase fees and complication. The problems we raise serve as a primer for what companies need to know about India's new rule and global data protection policy. Knowing these concerns can help digital enterprises plan ahead, meet future restrictions, and enter or depart markets. Fundamental privacy In 2017, India's Supreme Court decided that privacy is a constitutional right. Every digital citizen leaves a trail of private data. DPB controls the collection, security, storage, sale, and use of this data to preserve people' privacy rights. New restrictions would disrupt the cost-benefit calculations of many internet enterprises that offer free services yet profit from selling consumer data. If they can't gather, utilise, hold, and sell user data as profitably as previously, many digital corporations will have to reconsider their business models. Authorization DPB compels digital companies to get user permission before collecting personal data. It must describe data collection's scope and purpose. Each level of data processing requires explicit consent. Digital firms not only gather personal data, but also process it to produce new information that doesn't belong to the original user. Uber analyses traffic patterns while Amazon reviews customer comments. Raw data might be sent to a third-party data processor for processing, producing new information with other data collectors' data. Companies must rethink data monitoring and security practises and choose when and how to gain user rights. Digital firms become data fiduciaries under the DPB when they gain user authorization for initial data collection and subsequent processing. Data ownership DPB suggests that data providers own their personal data. This basic concept might be difficult to implement for digital firms. A property owner can request their property in the real world. Digital companies would have to comply with this rule when a user wants erasure or recall of their personal data, such as when a Facebook user requests deletion of all their information. Digital enterprises must also consider if they sold their data to a third party. Data types DPB has identified three data types for identifying principals. Financial, health, sexual orientation, genetic, transgender, caste, and religious data are sensitive. Military or national security data are examples of critical government data. Third is a generic category with undefined data. DPB specifies storage and processing requirements for each data class. Sensitive data must be housed on Indian servers. Sensitive data might be processed abroad but stored in India. Important data can't be exported. General data are unrestricted. Digital organisations store and process their data wherever it's most efficient.