EXPRESS COMPUTER

Navigating the data privacy landscape: Compliance strategies in a changing world

By: Vishal Salvi, CEO, Quick Heal Technologies Limited

The recent enactment of the Digital Personal Data Protection (DPDP) Act has undoubtedly marked a defining moment in India's technological trajectory, signifying a resolute commitment to securing citizens' rights in the digital age while also bolstering the nation's cybersecurity infrastructure. As we delve deeper into the implications of this legislation, it becomes evident that the DPDP Act is not just a legal framework; it is a strategic move that takes into account the rapidly evolving digital landscape of India. Apart from improving the governance and protection of citizens' personally identifiable information, the DPDP Act will also help the country leapfrog into a mature cybersecurity regime.

For many years, the attack surface vulnerability understanding and protection have been key focus areas in the cybersecurity domain. However, in recent times, the attack surface data proliferation has also become equally important. With the advent of big data and AI, organisations have been hoarding humungous amounts of data with the hope to monetise it in the future with diminishing ownership and accountability with its internal business owners. This has led to many high-profile incidents across the world and hence the provisions of the DPDP Act will not only establish accountability for misuse of personal data but also help organisations reduce their attack surface by enforcement of data retention and purging policies.

Privacy and cybersecurity domains have had their own trajectory during the exponential rise of digital adoption in the past two decades. While privacy focuses on the rights to maintain confidentiality and control over individuals' personally identifiable information, cybersecurity has primarily focused on unauthorised access, tampering, and disruption of information for

individuals or entities. Privacy deals with the protection of individual rights on their data by establishing accountability on entities. So, it's primarily a domain focused on compliance with the law of the land which is the DPDP or GDPR. Cybersecurity, on the other hand, is a domain focused on managing the cybersecurity risks due to the external/internal threat actors who are motivated to steal or disrupt your digital assets. The interesting part is that both these domains have a significant symbiosis with each other and hence my enthusiasm that with the DPDP, we should expect a significant shift in the maturity of the cybersecurity practices in our country.

While India has had the IT Act for more than two decades now, and the likes of banks, capital markets, insurance, etc. have been enforcing robust cybersecurity regulations for many years, these are quite sectoral and therefore, not able to impact the entire country. The enforcement of all the technical controls to achieve privacy are a part of the cybersecurity domain. Be it discovery, classification, protection, monitoring, and disposal. We have an advantage of many learnings from the implementation of similar regulations across the globe. Therefore, we can implement this more efficiently and optimally.

At its core, the DPDP Act is designed to regulate the entire lifecycle of personal data, encompassing its collection, processing, storage, and disclosure by a diverse array of entities spanning both the public and private sectors. This holistic approach reflects the recognition that the realms of privacy and security are inextricably intertwined. The act empowers individuals with an array of rights, ranging from the fundamental right to access and correct their data to the more nuanced right to data portability. A significant stride made by the DPDP Act is the establishment of a dedicated Data Protection Authority, entrusted with the monumental task of enforcing the act, mediating disputes, and imposing penalties for violations. This authority ensures that the legislation isn't just a theoretical construct but a living, breathing entity with real teeth.

Moreover, the DPDP Act positions India within a global framework, drawing lessons from the European Union's General Data Protection Regulation (GDPR). India's digital market is projected to reach a market value of $1 trillion by 2025. This robust growth accentuates the need for a fortified cybersecurity foundation to inspire investor confidence and ensure sustainable digital development. As we navigate this new chapter in our digital journey, it is imperative that both government bodies and private enterprises collaborate to ensure seamless implementation. With the right trajectory, India stands poised to not only overcome its cybersecurity challenges but also to emerge as a global exemplar in data protection.

The DPDP Act isn't merely a legal statute; it is a declaration of India's intent to safeguard its citizens' digital autonomy while fostering a secure environment for innovation and growth. Today, India has immensely vibrant talent in the cybersecurity market, not just for the country but also for the globe. The introduction of the DPDP Act is a momentous occasion that creates a great opportunity for India to be on the list of the safest nations in the world for conducting digital business. Let us embrace this with sharp focus and intent to make our country and its citizens' digital future safe and trustworthy.