Navigating data privacy amid ethical challenges in digital age

BY AMIT KIRTI
EY GDS Strategy and Transactions (SaT) Deals Technology and Analytics Leader

In the digital era, data has become the cornerstone of organizations a catalyst for growth, innovation and enhanced customer experiences.

As businesses increasingly depend on data, the importance of safeguarding data privacy has risen, presenting a myriad of challenges and opportunities for organisations to strengthen their ethical foundations. In our interconnected world, countless examples of colossal data breaches have resulted in financial losses, reputational damage, legal issues, regulatory penalties and a profound erosion of consumer trust.

As organisations navigate this ethical minefield, the importance of data privacy cannot be overstated. It transcends compliance – it is about preserving the trust that customers and employees place in the organizations.

Key strategies for organizations to fortify protection

Today, safeguarding data privacy demands proactive measures from organisations. Implementing technological fortifications such as robust firewalls and advanced encryption methods are critical. These measures not only deter external threats but also convince users that their data is managed with the utmost care and is protected.

Internal systemic initiatives are key for ingraining data privacy into organisational practices. Conducting regular audits to identify vulnerabilities, implementing stringent access controls and fostering a culture of responsibility within the organisation are vital. Integrating artificial intelligence (AI) for anomaly detection and real-time monitoring is now standard practice, enabling organisations to pre-empt potential threats effectively.

As organisations collaborate with third-party vendors that often have access to sensitive data, they must enable strict adherence to data privacy standards through contractual obligations, routine audits, and due diligence. Additionally, establishing an effective data breach incident response plan and conducting regular testing is also critical.

Further, organisations should consider adopting a comprehensive data governance framework. This involves defining clear policies and procedures for data handling, ensuring regulatory compliance and establishing accountability at all levels of the organisation. According to a Verizon 2023 Data Breach Report, a staggering 83% of breaches involve external factors, often driven by financial motives. Additionally, the human element is implicated in 74% of breaches, encompassing social engineering attacks, errors, or misuse.

Onboarding talent in the era of data privacy

Recognising the complexities and challenges posed by data privacy, organisations must prioritize investing in talent with specialised expertise in this domain. Beyond only compliance, it involves cultivating a culture of accountability and responsibility. Professionals who are wellversed in the intricacies of data privacy regulations can adeptly navigate the legal complexities, so that organisations not only adhere to standards but also surpass them.

Effective and efficient onboarding involves training employees with knowledge on being vigilant custodians of data, understanding the legal nuances and advocating for privacy protection. It is about cultivating a workforce that views data protection not only as an obligation but as a collective responsibility ingrained in the organisational ethos.

Organisations should also consider appointing a Chief Privacy Officer (CPO) or establishing a dedicated privacy team. This specialized role helps in data privacy remainingas strategic priority, with an executive-level individual overseeing compliance efforts, mitigating risks and driving a privacy-centric culture across the organization.

Privacy for trust: acornerstone principle

At the core of the data privacy discussion lies the fundamental principle of 'privacy for trust.' Whether customers or employees, users entrust organisations with their data. This trust acts as the linchpin that sustains business operations and nurtures growth. Just as customers are the lifeblood of any organisation, their trust serves as the lubricant that keeps the business machinery running seamlessly.

Transparent and lawful data collection practices, explicit consent procedures and empowering users with control over their personal data are indispensable principles of privacy. For examples, the seemingly mundane cookie settings on organisational websites are not merely pop-ups but critical mechanisms that uphold user autonomy while ensuring compliance with data privacy regulations. There have been several incidents involving government agencies and educational institutions in Sri Lanka where sensitive data, including personal and academic records, were exposed due to inadequate security measures.

In 2023, the email network of the Sri Lanka government itself was affected by a ransomware attack that wiped months of data from thousands of email accounts. This included data belonging to top government officials.

In 2020, a series of cyber attacks occurred on at least five Sri Lankan national websites on.gov and .com domains. The cyber attack also targeted a leading news website of Sri Lanka, compromising sensitive data. These data breaches highlight the growing threat landscape in Sri Lanka and the urgent need for stronger cybersecurity measures and data protection regulations.

Stronger compliance standards to navigate the future

While data privacy remains a challenge globally, the rapid expansion of digital technologies in Sri Lanka has brought about both opportunities and ethical dilemmas regarding data privacy. As the country embraces digitalisation across various sectors, including finance, healthcare and governance, the need to safeguard personal information has become paramount.

However, enabling data privacy has significant challenges. As in most countries, the lack of comprehensive data protection laws in Sri Lanka is an area of concern. While the country has taken steps to enact legislation such as the Data Protection Bill, it should be accompanied by steps to fill any regulatory gaps in implementation and enforcement. Just as in other countries, Sri Lanka too needs to adopt comprehensive data protection legislation aligned with international standards. Also, there is a need for awareness to empower individuals to understand and assert their privacy rights in the digital realm, especially because the proliferation of social media platforms and digital services has led to the collection and exploitation of vast amounts of personal data without adequate consent or transparency.

As data privacy laws, regulations and standards see continuous evolution on a global scale, organisations must prepare for more stringent and demanding compliance practices. The formidable task at hand extends beyond mere avoidance of fines and penalties; it revolves around preserving customer trust, confidence and upholding ethical integrity.

In this era where data serves as both an asset and a potential liability, organisations that prioritise data privacy will emerge as ethical leaders. The focus must transition from 'privacy by design' solely for compliance purposes to 'privacy by default,' ingraining and embedding data protection as a core value of organisational culture. In doing so, organisations can embark on a journey where data privacy is not merely a checkbox on a compliance list but looked upon with a sense of duty and responsibility.

The views reflected in this article are the views of the author and do not necessarily reflect the views of the global EY organization or its member firms.