Q: We are a financial services organization. There are new regulations with which we need to comply that state we must adopt privacy by design. Can you further define privacy by design?

A: Privacy by design is a framework based on proactively embedding privacy into the design and operation of IT systems, networked infrastructure and business practices.[1]

Privacy by design is a methodology originally developed in 1995. It takes a broad view of a system and its data relative to seven principles:

1. **Proactive not reactive; preventive not remedial**—This principle encourages organizations to perform risk assessments and identify events that may impact data privacy instead of waiting for breaches to happen and then reacting to fix issues. The focus is on preventing the privacy-related risk from materializing.
2. **Privacy as the default setting**—Setting default rules for privacy data protection helps prevent breaches. This principle asserts that the individual is not required to do anything to protect privacy; the system protects it. The basic privacy principles include purpose for collecting privacy data, method and limitations for collection to minimize privacy data and defining use, retention and disclosure requirements.
3. **Privacy embedded into design**—Privacy should be an integral part of system design and not an add-on feature. This can be achieved by adopting global standards and performing risk assessments that include privacy-related risk, for example, adding a classification of "Privacy" in data and assets classification schema and creating awareness among system users.
4. **Full functionality; positive-sum, not zero-sum**—This approach helps ensure privacy compliance without impairing the product and service functionalities. When organizations consider privacy as add-on, it is zero-sum; however, when all requirements such as privacy, security, processing and retention are considered together, it is positive-sum.
5. **End-to-end security; full life cycle protection**—This principle emphasizes protecting privacy data throughout their life cycle, from data origination to data destruction, including storing, processing and dissemination. This principle, along with positive sum, helps secure privacy without affecting service delivery. This ensures that organizations assume responsibility for protecting data privacy, as well as additional security required by compliance requirements such as encryption, anonymization and data masking.
6. **Visibility and transparency; keep it open**—The organizations collecting and processing privacy data are accountable for protecting those data, acting with transparency about what happens with the data and monitoring compliance. This

"Privacy should be an integral part of system design and not an add-on feature."

SUNIL BAKSHI | CISA, CRISC, CISM, CGEIT, CDPSE, AMIIB, MCA

Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant in India.

principle focuses on the basic privacy principles of accountability, openness and compliance.

7. **Respect for user privacy; keep it usercentric**—This principle asserts that organizations must demonstrate respect for the privacy of data subjects and take into consideration data subjects' expectations while collecting, processing and storing privacy-related data. This involves implementing processes for obtaining consent from data subjects, ensuring the accuracy of privacy data, determining access levels for users and ensuring compliance.[2]

Adopting all these practices requires:

- A clear commitment to and leadership by senior management and the board of directors (BoD) to set and enforce high standards of privacy
- A privacy commitment that is shared openly throughout the organization by user communities and stakeholders in a culture of continuous improvement
- Established processes to identify and rectify issues in privacy designs, privacy practices and outcomes to avoid any negative impacts well before they occur

Privacy by design helps organizations ensure a holistic approach toward privacy-related compliance.

Endnotes

1 Deloitte, *Privacy by Design: Setting a New Standard for Privacy Certification,* USA, h*ttps://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF*

2 Cavoukian, A.; *Privacy by Design—The Seven Foundational Principles,* International Association of Privacy Professionals (IAPP), USA, 2010, *https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/*