Q: I am a CISO of a multinational organization. There are multiple regulations and laws requiring protecting the privacy-related data of customers and stakeholders. As a regulated entity, we also need to disclose some information to regulators that might result in noncompliance with privacy-related regulations. What should we do to address this issue?

A: This is a common dichotomy faced by security managers. Privacy-related regulations and laws require protecting customers' privacy-related information and, at the same time, some regulations require sharing such information with authorities. Compliance with one regulation resulting in noncompliance with another.

Many countries have not yet enacted privacy-related laws and, if an organization is operating in such a location, it faces compliance issues. Organizations need to understand the priorities of compliance. It is an accepted principle that a multinational organization needs to comply with local laws first and then global laws. Global laws require compliance with privacy-related regulations, but may be unaware of the fact that local authorities may require organizations to provide an individual's privacy-related data. The dilemma then is can the organization deny providing such information? It may result in noncompliance with global policies.

Organizations collect personal data to provide services to customers and stakeholders. Such data need to be protected from any kind of breach to protect the customer's information. These generally accepted principles are covered by most privacy-related regulations:

- **Notice**—Data subjects should be given notice when their data are being collected
- **Collection**—How are the data collected from data subjects?
- **Purpose**—Data should only be used for the purpose stated and not for any other purposes.
- **Consent**—Data should not be disclosed without the data subject's consent.
- **Security**—Collected data should be kept secure from any potential abuses.
- **Disclosure**—Data subjects should be informed as to who is collecting their data.
- **Quality**—Organizations are responsible for maintaining the quality of privacy-related data.
- **Access**—Data subjects should be allowed to access their data and make corrections to any inaccurate data.
- **Accountability**—Data subjects should have a method available to them to hold data collectors accountable for not following the principles stated herein.
- **Retention**—Many regulations specify the retention limits of privacy-related data of data subjects.

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
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.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2BZdKFD

There may be a few more compliance requirements with respect to specific regulations. However, most regulations make exceptions to compliance on the grounds of national security.

The conflict occurs when local governments or judicial authorities request data related to customers for national security purposes and the organization may have to provide such data resulting in noncompliance with the regulations of the country of origin of the organization.

> MANY COUNTRIES HAVE NOT YET ENACTED PRIVACY-RELATED LAWS AND, IF AN ORGANIZATION IS OPERATING IN SUCH A LOCATION, IT FACES COMPLIANCE ISSUES.

In this situation, organizations need to assess the risk associated with noncompliance with respect to local compliance requirements *vis-à-vis* that of corporate compliance requirements and formulate privacy polices defining such exceptions. Ideally, the policies should provide for informed consent from data subjects and mandatory notice to the data subjects in cases of sharing information with authorities. Organizations must ensure that these exceptions and policies are communicated to data subjects while collecting the privacy-related data.

Another situation may arise where organizations in a service sector such as banks, insurance companies or e-commerce, follow a common practice to profile customers. Profiling customers requires collecting transaction data of customer behaviors, which amounts to monitoring individuals. In these cases, organizations must obtain exclusive informed consent from data subjects.

Organizations also need to take care when sharing customer data with vendors for processing. Weak security practices of vendors and inappropriately worded clauses in vendor contracts can result in data breaches. In certain situations, it is necessary to inform data subjects and authorities of breached data. Vendor monitoring and periodic auditing of vendors may help.