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.

http://bit.ly/2B0Ktus

Q The European Union (EU) General Data Protection Regulation (GDPR) will take effect in May 2018. My organization is not doing any business in Europe currently, but we have plans to expand. How will GDPR affect us? Will it affect us if we do not have an office in Europe?

A GDPR (Regulation [EU] 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union. It also addresses the export of personal data outside the European Union for processing. The primary objective of the GDPR is to give assurance to EU citizens that their personal data are processed in a secure environment and have adequate legal protection. The regulation was adopted on 27 April 2016. It will be enforceable beginning on 25 May 2018 after a two-year transition period. Unlike a directive, it does not require any enabling legislation to be passed by national governments; thus, it is directly binding and applicable.

An important aspect of GDPR is that it applies to organizations that are not part of the European Union but collect and/or process personal data of EU residents outside the EU's geographical boundaries. Although the regulation does not apply to the processing of personal data for national security activities or law enforcement, it has a separate Data Protection Directive for the police and criminal justice sector that provides rules on personal data exchanges at the national, European and international levels.

The term "personal data" refers to any information relating to an individual's private, professional or public life. It includes the individual's name, home address, photo, email address, bank details, posts on social networking websites, medical information, or IP address of a personal device.[1]

The new EU data protection regime extends the scope of the EU data protection law to all foreign organizations processing the data of EU residents. It provides for a harmonization of the data protection regulations throughout the European Union, thereby making it easier for non-European companies to comply with these regulations. However, this comes at the cost of a strict data protection compliance regime with severe penalties of up to 4 percent of worldwide turnover or upper limit of £20 million, whichever is higher.[2]

Some facts about GDPR include:[3]

- If a business is not in the European Union, it still must to comply with the regulation if it is processing the personal data of EU citizens outside the EU's geographical boundaries.
- The definition of "personal data" is broader, bringing more data into the regulated perimeter.
- Consent will be necessary for processing children's data.
- The rules for obtaining valid consent have been changed.
- The appointment of a data protection officer (DPO) will be mandatory for certain organizations.
- Mandatory data protection impact assessments (technical as well as privacy assessments) have been introduced.
- There are new requirements for data breach notifications.
- Data subjects have the following rights:
  - Right to be forgotten/erasure
  - Right to access
  - Right to rectification
  - Right to object
- There are new restrictions on international data transfers.
- Data processors share responsibility for protecting personal data, along with the data controller.
- There are new requirements for data portability.
- Processes must be built on the principle of privacy by design.
- The GDPR is a one-stop shop.

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999 LI, 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 and visiting faculty member at the National Institute of Bank Management, India.

Therefore, if an organization needs to process EU citizens' personal data while offering goods or services to those citizens (data subjects), the organization is a data controller and is subject to GDPR regulation, regardless of whether the organization is based inside or outside the European Union. If an organization does business with data subjects in the European Union, the organization needs to comply with the EU regulation, even if the services or goods provided do not involve connecting to a payment system.

According to some experts, the wording "data subjects who are in the European Union" indicates that the GDPR covers the data of EU citizens as well as temporary residents and even those on vacation.[4] It may also be interpreted that EU citizens traveling outside the European Union whose data are collected and processed outside the European Union may not be subject to GDPR regulation.[5]

The "territorial scope" clause does not mean that every single web-based business that is accessible from within the European Union is in scope of the GDPR. The fact that someone in the European Union can visit an organization's website does not automatically bring that website into "territorial scope." The website has to be doing something to actively reach out to someone in the European Union.[6]

An organization may be exempt from GDPR compliance in the following situations:[7]

- If the processing of personal data from EU-based data subjects is occasional or not on a large scale
- If the personal data to be processed do not include special categories of personal data or relate to criminal convictions and offenses
- If the nature, context, scope and purposes of the processing are unlikely to result in a risk to the rights and freedoms of the data subject

In all other cases where the "territorial scope" extends to non-EU-based organizations that process the data of persons from the European Union (data controllers), organizations will need to nominate an EU representative within the European Union.[8] Some conditions relating to that representative include:

- The EU representative is the first point of contact for the data protection supervisory authorities and data subjects. The contact information for the EU representative of an organization and its contact information must appear on the organization's website along with terms of service between the organization and the EU representative.
- The EU representative must be located in a member state in which the organization's EU data subjects are based. If the organization targets the entire European Union, then the EU representative may be based in any member country.
- The EU representative must operate under the organization's direction and the directions must be in writing. The legislation does not specifically state "under contract," but it is fairly safe to assume it may be in the contract.
- The EU representative will be designated "without prejudice" to legal actions that may be taken against the data controller or the data processor. An organization cannot outsource accountability toward the data subjects to its EU representative.

Author's Note

The views expressed here are the author's. For more detailed understanding, consult a legal expert.

Endnotes

1 For this definition and definitions of other pertinent terms, such as "processing," "restriction of processing," "profiling" and "pseudonymization" (some experts refer to it as "tokenization"), see *https://gdpr-info.eu/art-4-gdpr/*.
2 *IT Governance, Data Protection Act (DPA)* and *EU GDPR Penalties*, *https://www.itgovernance.co.uk/dpa-and-dgpr-penalties*
3 IT Governance, The EU General Data Protection Regulation, *https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation*
4 Murphy, M.; "Rules of Establishment for European Data Controllers and Data Processors," Safe Data Matters, 3 August 2016, *http://safedatamatters.com/gdpr-datacontrollerspart2-establishment/*
5 *Ibid*.
6 *Ibid*.
7 *Ibid*.
8 *Ibid*.