Lesson 4 | Data Protection by Design and Default

Updated 2020-09-21

One of the areas of GDPR that has gotten a lot of attention is the concept of Data Protection by Design and Default. This concept is outlined in Article 25 of GDPR.

The concept of data protection by default and design can be broken down into two areas.

1. **Security by default**. Paragraph 1 of Article 25 mandates that organizations implement the appropriate technical and organizational controls in order to meet the requirements of this Regulation and protect the rights of data subjects. This is the implementation requirement.
2. **Privacy by default**. Paragraph 2 of Article 25 mandates that organizations only collect, process, and store the personal information required for the specific purpose of processing.

There is an overlap between the areas of privacy and security in how GDPR requires aspects of both. The overarching message is that organizations, in order to comply with GDPR, need to design a program to minimize data collection and processing to the minimum necessary data, and then they need to implement security, both technical and organizational, to protect that minimum amount of data. These requirements are far-reaching within an organization.

GDPR mandates privacy policies and procedures for personal data collection and security implementations to protect personal data.