# GDPR: Not Just an IT Issue

The EU's General Data Protection Regulation (GDPR) imposes new rules on organizations in the European Union (EU) and those that offer goods and services to people in the EU and European Economic Area (EEA), or that collect and analyze data tied to people in the EU/EEA, no matter where the organizations are located.

## An Involved Organization

Compliance with GDPR requires the involvement of people, processes, and technology across the organization.

### PEOPLE

Competent resources, staff training, and executive commitment.

### TECHNOLOGY

Identify, protect, and manage your data.

### PROCESS

Data governance, subject access requests, breach notification, and best practices.

## Where to Begin

GDPR compliance is a journey and full compliance takes resources, commitment, and time.

### ASSIGN RESPONSIBILITY

Understand the Regulation, determine if it applies to your organization, and don't go at it alone (work with an expert).

### LAWFUL BASIS OF PROCESSING

Determine and document the lawful basis for your processing activities under GDPR.

### DATA PROTECTION OFFICER/ EU REPRESENTATIVE

Determine if you are required to appoint a Data Protection Officer.

### RECORDS OF PROCESSING

Document the required information as stipulated by GDPR and put a plan in place to maintain this information.

### ASSESS AND DISCOVER

Assess your posture against the Regulation. Identify the type, category, and location of the data you process. Create a data inventory and data flow diagram.

### PRIVACY NOTICES

Review current privacy notices and put a plan in place for making any necessary changes for GDPR compliance.

### SUBJECT ACCESS REQUESTS

Establish procedures for addressing requests from your data subject, keeping in mind the one-month time constraint.

### DATA BREACH NOTIFICATION

Review your current breach notification process and put a plan in place to adhere to the 72-hour requirement.