

What is the GDPR?

The General Data Protection Regulation (GDPR) is a new data protection framework that governs how organizations collect, process, and use personal data across all 28 EU member states. The GDPR takes effect in May 2018 and imposes new rules on organizations in the European Union (EU) and those that offer goods and services to people in the EU, or that collect and analyze data tied to people in the EU, no matter where the organizations are located.

One Set of Rules

for all companies collecting, storing, or using the personal data of people in the EU

Penalties for Non-compliance:
Up to 4% of last year's global sales or **€20 million**, whichever is greater

Applies to 100%

of companies that collect or process personal data of people in the EU, even if the data is stored or used outside the EU

72 Hours —

Time in which data breaches must generally be reported to supervisory authority

DPO Required — Many businesses are required to appoint a **Data Protection Officer**, including those processing high volumes of personal data



The GDPR gives consumers more control over the collection, processing, and retention of their personal data:

Consumer Rights

- The **RIGHT** to withdraw consent and have all data removed
- The **RIGHT** to correct errors
- The **RIGHT** to be notified if data is endangered
- The **RIGHT** to request data in a portable format and to transfer data between companies

Company Responsibilities

- The **RESPONSIBILITY** to minimize data collection
- The **RESPONSIBILITY** to limit processing to the purpose for which data was collected
- The **RESPONSIBILITY** to conduct proactive assessments when processing consumer data
- The **RESPONSIBILITY** to record data processing activities and limit who can access consumer data
- The **RESPONSIBILITY** to report breaches without undue delay, typically 72 hours
- The **RESPONSIBILITY** to be transparent about what personal data they collect and how it is used



GDPR enforcement begins

92% of US organizations

say GDPR compliance is a top data protection priority

Source:
<https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-gdpr-series-pulse-survey.pdf>

77% of US companies

with more than 500 employees plan to spend at least \$1 million on the GDPR

Source:
<https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html>

69% of companies

say they plan to use a technology firm to help with the GDPR preparations

Source:
<https://www.pwc.com/us/en/increasing-it-effectiveness/publications/general-data-protection-regulation-gdpr-budgets.html>

Compliance 101

Communicate

Use plain language to tell people who you are, explain why you need their data, how long it will be stored, and how it will be shared.

Get Consent

When required, obtain clear consent to data collection, and check age requirements for parental consent.

Provide Access

Allow people to access their data in a portable format, make corrections, and transfer it to other companies if they choose.

Warn & Protect

Provide notice of breaches when consumer data is at risk, and understand limits on processing special categories of sensitive data.

Opt-Out & Remove

Give people the opportunity to opt-out of direct marketing that uses their personal data and delete their data when they exercise their "right to be forgotten."

Profiling

If you use data profiling to process applications for legally-binding agreements, you must inform consumers, provide a manual check of the process, and allow applicants to contest the decision if an application is denied.

Privacy Risk Assessment

Processing or storing data with a high risk to the privacy or rights of people in the EU? GDPR requires you to conduct a Data Protection Impact Assessment.

Sensitive Personal Data

The GDPR has heightened requirements for processing highly sensitive personal data, including:

- Race or ethnicity
- Political, religious or philosophical beliefs
- Health information
- Sexual preferences
- Trade union membership

How to Get Started

Learn

Take advantage of our GDPR Foundations Training to learn more about requirements.

Assess

Complete our GDPR Readiness Assessment to determine how to proceed.

Plan

Work with our security and compliance experts to develop a GDPR roadmap for your organization.

Contact us to learn more about how we can help simplify the impact of the GDPR on your organization.

Technology Management Concepts
www.abouttmc.com | info@tmc-la.com

t [m] c TECHNOLOGY MANAGEMENT CONCEPTS
A Microsoft Dynamics™ Partner

*This information is a commentary on the GDPR, as Microsoft interprets it, as of the date of publication. Application of GDPR is highly fact-specific, and not all aspects of GDPR are well-settled. This information should not be relied on as legal advice.