BARR ADVISORY

A QUICK GUIDE TO
GDPR COMPLIANCE

Companies around the world face a steep climb to GDPR compliance. Use this guide to become as compliant as possible, safeguard EU data and avoid losing revenue.

What is **GDPR**?

The new General Data Protection Regulation (GDPR) will standardize and strengthen data protection for individuals within the European Union.

25
GOES INTO EFFECT
MAY 25, 2018
ARE YOU READY?

Who does this apply to?

All public and private organizations that handle, store or process personal data of EU citizens.

Also applies to non-EU companies if they process personal data of individuals in the EU.

Did you **know?**

About **⅓ of global companies** don't know whether they need to comply with GDPR.

Cloud service providers will be held responsible as "data processors" under GDPR.

**Compliance Isn't Cheap:
68 percent** of affected U.S. companies anticipate costs of **more than $1 million.**

Steep penalties
for non-compliance and breaches

Fined up to **4%** of annual global revenue or

€20 million, whichever is greater

Deadline to tell authorities about data breach:

72 hours

Must tell users: **"without undue delay"**

Don't think of GDPR as the framework.
Instead, build a new one in 4 steps.

1

MAP OUT DATA FLOWS

Ask yourself, "Do we have EU data?" If the answer is "no," then the next question becomes "Are we sure we are not collecting EU data and will not in the future?" With those questions answered, designate someone within the organization to map and maintain data flows.

2

REDUCE THE SCOPE

Define what data is considered protected by the EU, and then use data discovery or loss protection and prevention tools to scan the environment for various rule sets on protected data.

3

PERFORM A GAP ANALYSIS

Where does the company collect and store large quantities of data, how is that information stored, and what are the risks of breach or improper use of information? Work down from the area of highest risk to tackle pressing issues first.

4

DESIGNATE A PRIVACY OFFICER

Compliance isn't a one-time event. Create a committee to assess compliance on a monthly or quarterly basis. By starting with a group, the person who should be in charge will emerge naturally over time.

Source: https://cloudtweaks.com/2017/11/quick-dirty-guide-gdpr-compliance/

barradvisory.com
info@barradvisory.com