

GDPR

For Dummies

General Data Protection Regulation



25 May 2018

The GDPR is already in effect.

Penalties for noncompliance are up to €20 million (\$23 million) or 4% of annual global turnover.

The GDPR was passed by the European Union (EU), but applies to any company worldwide that targets EU users.

What is it?

The GDPR is a ground-breaking privacy law that regulates how companies collect, handle, and protect personal data.

Personal data is worth trillions of dollars – in the digital age, it's like oil. Strict legislation ensures companies process it responsibly.

Does my business need to comply with the GDPR?

Do you have customers in or collect data from users in the EU?

YES The GDPR applies to you. Time to comply.

NO You're in the clear. Put your feet up.

I DON'T KNOW Get out of here and find out...

What is personal data?

Personal data is any information shared online that can be used to identify an individual.

It's like a jigsaw – when the pieces are put together, they reveal a vivid picture of a person's life.

Name

Phone number

Address

Date of birth

Bank account

Passport number

Location

Health records

Race

Political opinions

Religious views

Social media posts

Sign Up

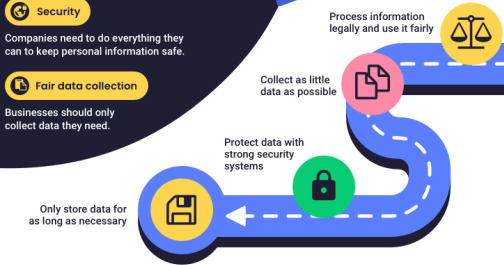
Users now have the right to...

- Learn how their data is used
- Find out what companies already know about them
- Correct mistakes in their data
- Have their data deleted
- Refuse data processing

Key GDPR concepts

- Consent**
Companies must ask for permission to process personal data and should explain their practices in clear and simple language.
- Privacy by Design**
Privacy and respect for users' data should be a company's default setting.
- Security**
Companies need to do everything they can to keep personal information safe.
- Fair data collection**
Businesses should only collect data they need.

How to comply



Privacy policy
You need one of these to explain how you process data, so users can agree (or not).

Data breach
The formal name for when data is lost, stolen, destroyed, or changed.

72 hours
That's how much time you have to report a data breach to your supervisory authority.

Data protection impact assessments (DPIAs)
Fill out one of these if your data processing activities are high risk – as in they could pose a risk to someone's freedom.

Who's who

- Data subject**
Anyone who has their data collected.
- Data controller**
The business/organization that collects the data.
- Data protection officer (DPO)**
The person who handles GDPR paperwork for a company.
- Supervisory authority**
An organization in each EU country that enforces the GDPR in their region.

If the GDPR applies to your business,

You Need to Comply NOW

Don't be a dummy and treat data privacy as an afterthought. Take the steps now to comply with the GDPR and save your business from huge fines and potential meltdown.