
# The General Data Protection Regulation (GDPR)

What you need to know about the new regulation for personal data protection

# What is the GDPR?

- The General Data Protection Regulation (GDPR) is a new privacy law that gives residents of the European Union greater control over their “personal data” and requires organizations to maintain appropriate security of personal data.

- **Objectives:**
  - Update the old Data Protection standards (Oct 1995) to fit today’s technology
  - Harmonize data privacy laws across Europe
  - Boost the digital market by restoring the confidence of Europeans about data collecting
    - According to the European Commission, more than 90% of Europeans are concerned about mobile apps collecting their data without their consent

# Timelime

**2012**

- The European Commission proposed to **reform** the current fragmented legal framework to deal with the new challenges for the protection of personal data and to make the EU member states fit for the digital age.

**2016**

- On 4 May 2016, the **EU Regulation on Data Protection (GDPR)** has been published in the Official Journal of the European Union. The GDPR has entered into force on 24 May 2016 and will replace the former 1995 EU Data Protection Directive and create a harmonized data protection law across Europe.

**2018**

**WHEN? May 25th 2018**

- The GDPR will be enforced as from **25 May 2018** directly across all 28 EU Member States after a two years implementation period.
- But some countries will amend their local laws sooner. Watch out !

# Which types of data need to be protected?

**PERSONAL DATA**

Anything that allows a living person to be directly or indirectly identified

- Name
- Address
- E-mail
- Mobile number
- ID
- etc.

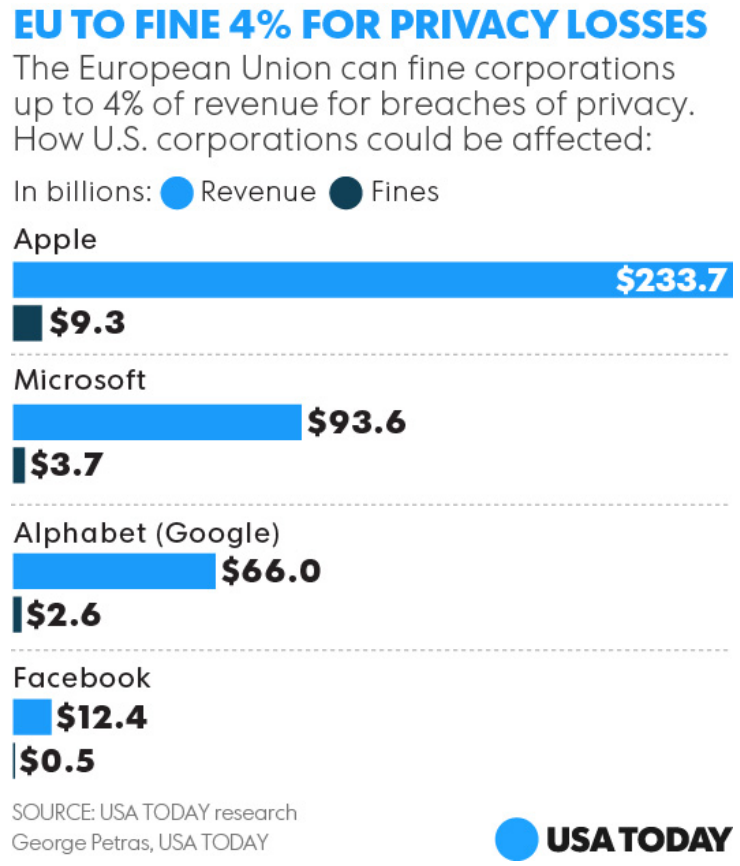
**SENSITIVE PERSONAL DATA**

‘Special categories' of information

- Religious beliefs
- Political opinions
- Race
- Sexual orientation
- Health information
- etc.

# Why should we care?

- GDPR applies to any company that offer goods or services on the EU that collect personal data of EU individuals.
- Companies that don’t comply will be exposed to serious fines. Whichever is greater:
  - Up to 4% of annual revenue
  - Up to €20M



# Key changes
## Individuals' Data Rights

- **Consent**
  - Stricter requirements on obtaining valid consent from individuals to justify the processing of their personal data.
- **Additional Protection for Children (< 16 years old)**
  - Only valid if authorized by a parent
- **Data Access Rights**
  - Right to Access
    - Right to obtain data that is being processed, where and for what purpose
  - Right to Rectification and Erasure ("right to be forgotten")
  - Right to data portability
    - Right to transfer personal data from one organization to another

# Key changes
## Data Protection

- **Data Protection by Design and by Default**
  - Companies must demonstrate an evidence that data security is embedded in products and services from the early development stage.
  - Only necessary personal data are processed.


- **Compliance Standards**
  - Compliance with the international information security standard ISO 27001.
- **Records of Data Processing**
  - Records need to contain a specific set of information so that it is clear what, where, how and why data is processed.

# Key changes
## Accountability

- **Breach notification**
  - Mandatory for an organization to report any data breach to its supervisory authority within 72 hours.
  - Individuals must be contacted in high-risk breaches
    - Not necessary if protective measures eliminate the danger immediately
- **Hire Data Protection Officer (DPO)**
  - Many organizations will be required to appoint a data protection officer (DPO)
  - A DPO must be appointed where:
    - The processing is carried out by a public authority
    - Regular monitoring of individuals on a large scale
    - Large-scale processing of sensitive personal data or data relating to criminal convictions and offences

# Recap…

- Companies that do business in the EU must **only process and store** customer data that is **absolutely necessary** to their business
- More **explicit consent** must be obtained from a customer before a business can collect their data
- Businesses must **report any suspected data breaches** within 72 hours
- Individuals have the **right to access** their data at any time, and the **right to be forgotten**
- Some businesses will be required to **hire a Data Protection Officer (DPO)**

# Final Thoughts

- **Challenges for implementing**
  - Team Compliance and Training
  - Implementing new data processing methods
  - Identifying and understanding how to deal with a data breach
  - Appointing a Data Protection Officer
- **Critics**
  - Less available data may stifle innovation
  - Small companies have less resources for implementing the changes
- **Opportunities**
  - Re-establish a relationship of trust with EU customers
    - Transparency can be an incentive for individuals to share their data more easily
  - Companies are hiring data protection professionals

# Resources

- **Regulation (EU) 2016/679:** http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en

- **GDPR Portal:** https://www.eugdpr.org

- **European Commission - Fact Sheet :** http://europa.eu/rapid/press-release_MEMO-15-5170_en.htm