

GDPR: KEY POINTS YOU NEED TO KNOW ABOUT THE REGULATION



'Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data'¹.

What is GDPR and when will it take effect?

The General Data Protection Regulation (Regulation (EU) 2016/679) represents a comprehensive reform of the EU's 1995 Data Protection Directive (Directive 95/46/EC). The regulation was adopted on 27 April 2016. It will come into force on 25 May 2018.

Main goals

The primary aim of the document is to provide citizens and residents of the EU with control over their personal data as well as to boost economic growth within the EU.

Who does the regulation apply to?

According to Art.3 GDPR, the regulation applies to

- EU-based data controller (entity that collects data from EU residents);
- EU-based processor (person or group that processes data on behalf of data controller e.g. cloud service providers);
- EU-based data subject (person);
- organizations based outside the EU, if they collect or process personal data of EU residents.

What are personal data?

'Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, your posts on social networking websites, your medical information, or your computer's IP address'².

Main requirements of the regulation

1

Personal data processing

(Art.5 GDPR)

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2

Lawfulness and consent

(Art. 6,7,8 GDPR)

Personal data processing shall be lawful. It means data subject should give explicit consent to data processing for one or more specific purposes. Furthermore, the data processing of a person below the age of 16 years requires a consent that is given or authorized by the holder of parental responsibility over the person.

3

Right of access

(Art. 15 GDPR)

The data subject has the right to obtain confirmation as to whether or not personal data concerning him or her are being processed, and the information on the purposes of the processing.

4

Right to erasure

(Art. 17 GDPR)

The EU citizens and residents have the right to obtain the erasure of their personal data.

5

Right to data portability

(Art. 20 GDPR)

The data subject has the right to receive the personal data that have been provided to a controller and to transmit these data to another controller.

6

Data protection and processing security

(Art. 25, 32 GDPR)

The controllers are obligated to implement appropriate technical and organizational measures to ensure that only personal data required for a specific purpose are processed. Measures that are applied as appropriate are clarified in Art.32 GDPR.

7

Data breach reporting

(Art. 33, 34 GDPR)

In the case of a personal data breach, the controllers are under a legal obligation to notify the data breach within 72 hours after having become aware of it to the supervisory authority and the data subject.

8

Impact assessment

(Art. 35 GDPR)

The controller is obligated to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. The assessment should contain inter alia, the measures envisaged to address the risks in order to ensure the protection of personal data and to demonstrate compliance with the Regulation.

9

Data protection officer

(Art. 37, 38, 39 GDPR)

The data controllers and processors must designate a data protection officer to ensure the compliance with the Regulation. According to Art.37, data protection officers must be appointed for all public authorities, and where the core activities of the controller or the processor include regular and systematic monitoring of data subjects on a large scale or where the entity carries out large-scale processing of special categories of personal data defined in Art.9.

10

Penalties for non-compliance

(Art. 83 GDPR)

In case a controller or processor fails to meet the requirements, the supervising authority has the power to take the following sanctions (Art. 58 GDPR):

- Issue warning
- Issue reprimands
- Order compliance with data subjects requests
- Communicate the personal data breach directly to the data subject

Additionally, there are 2 tiers of the administrative fine that can be imposed:

- Up to €10,000,000 or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater,
- Up to €20,000,000 or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

About Qulix

Qulix Systems is a global provider of software design and development, quality assurance and IT consulting services. Since the year of 2000, we aim at delivering high-quality software solutions meeting our clients' needs across multiple business domains. [Read more...](#)



Have questions? Feel free to contact us:
request@qulix.com