

At nearly 100 pages, and the subject of innumerable articles and analyses since its first draft debuted in 2012, the General Data Protection Regulation can be overwhelming.

Here's a high-level look at what the GDPR requires of organizations collecting or processing the personal data of individuals in the EU, what rights it grants to individuals, and what consequences exist for not complying with the regulation when it comes into force in May 2018.



## What consumers can do:

- Withdraw consent for processing
- Request a copy of all of their data
- Request the ability to move their data to a different organization
- Request that you delete information they consider no longer relevant
- Object to automated decision-making processes, including profiling



## What regulators can do:

- Ask for records of processing activities and proof of steps taken to comply with the GDPR
- Impose temporary data processing bans, require data breach notification, or order erasure of personal data
- Suspend cross-border data flows
- Enforce penalties of up to 20 million Euro or 4 percent of annual revenues for non-compliance



## What organizations have to do:

- Implement “Privacy by Default” and “Privacy by Design”
- Maintain appropriate data security
- Notify data protection agencies and consumers of data breaches
- Get appropriate consent for most personal data collection and provide notification of personal data processing activities
- Get a parent's consent to collect data for children under 16
- Keep records of all processing of personal information
- Appoint a Data Protection Officer (if you regularly process lots of data, or particularly sensitive data)
- Take responsibility for the security and processing activities of third-party vendors
- Conduct Data Protection Impact Assessments on new processing activities
- Institute safeguards for cross-border data transfers
- Consult with regulators before certain processing activities
- Be able to demonstrate compliance on demand
- Provide appropriate data protection training to personnel having permanent or regular access to personal data