Deloitte.

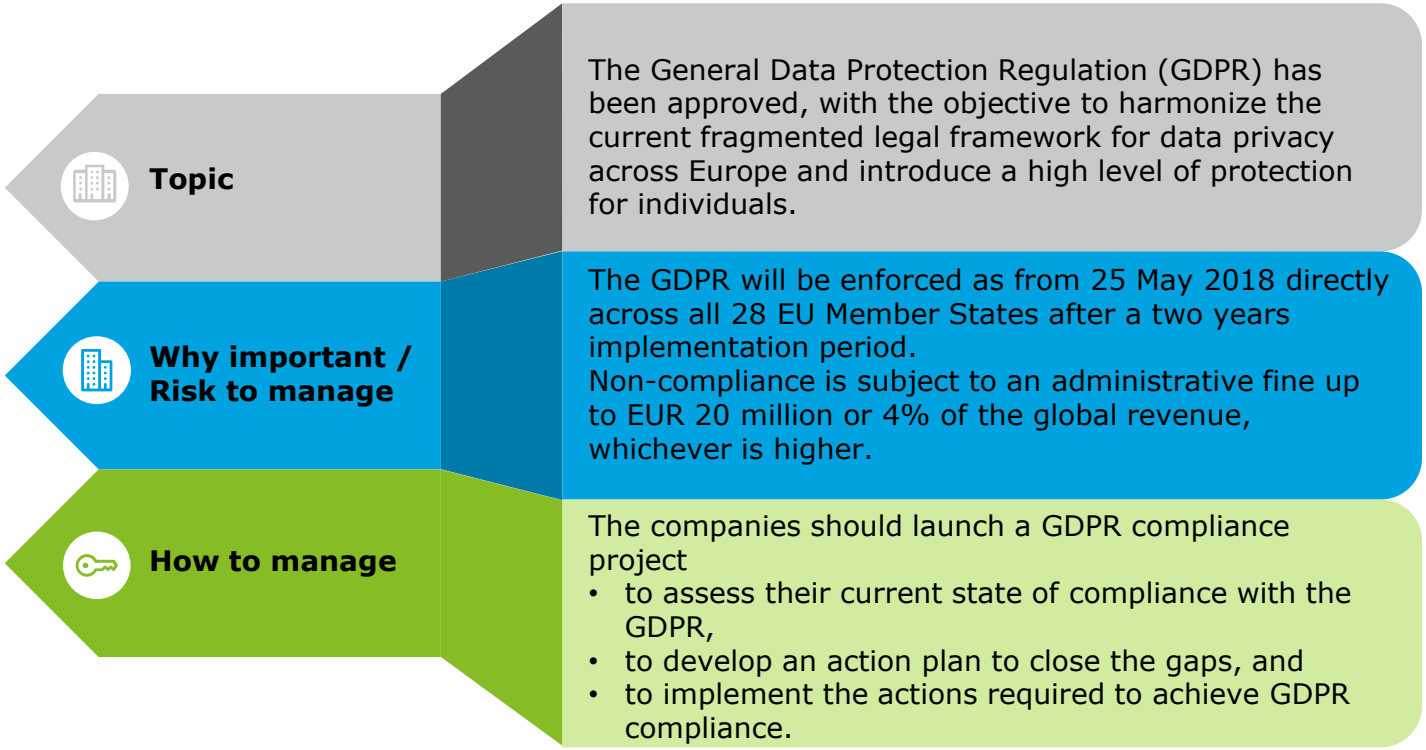
GDPR Advisory Services

October 2017

New EU wide General Data Protection Regulation

Final deadline

Compliance must be reached by 25 May, 2018



Quick GDPR Overview

Key changes

Broader territorial scope

- The regulation applies on a broader territorial scope which means that even if the data is not processed inside EU, as long as data subjects are EU citizens, the organization will have to comply in certain cases.

Significant increases in fines

- Failure to comply with the GDPR can result in heavy fines and restitution—upwards of 4% of your global revenue or €20m, whichever is higher. Other administrative measures may also be imposed such as deletion of client database in case of unlawful data processing.

Mandatory disclosure of data loss incidents

- If an organization loses personal data, it has 72 hours to inform the local regulator. At that point, information on the circumstances of the breach and the technical measures that were in place to safeguard the data must be given to the regulator. The individuals whose data has been lost must also be informed "promptly".

Increased powers of Data Protection Authorities

- Multinational companies will be regulated by the supervisory authority where they have their "main establishment". Data Protection Authorities (DPA) of main establishment can act as lead DPA, supervising processing activities throughout the EU (One-stop-shop). However, other "concerned" authorities may also be involved in handling complaints about them.

Quick GDPR Overview

Key changes

(Mandatory) Data Protection Officer

- Many organizations will be required to appoint a data protection officer (DPO) as a result of the GDPR.

Focus on accountability & transparency

- The new concept requires the companies the ability to demonstrate compliance with the GDPR, e.g. keep detailed records, implement appropriate technological and organizational measures.

Right to data portability

- Where the processing of personal data is carried out by automated means, Clients and employees will have the right to request and receive their own data in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another party.

International data transfers

- Data transfers to countries outside the EEA continue to be prohibited unless that country ensures an adequate
- level of protection.

Deloitte’s approach
GDPR Compliance Program