General Data Protection Regulation

Achieving GDPR Compliance

Journey to Data Privacy

Who has to comply

GDPR EU legislation is applicable to organisations either processing personal data in the EU, or relating to EU citizens.

The legislation applies to organisations inside and outside of the EU.

Non-compliant organisations may find it more difficult to do business in Europe.

GDPR EU legislation became law in 2016. The GDPR implementation date of 25th May 2018 is when the legislation is enforced.

Why GDPR

There are many regulations that relate to data privacy. GDPR harmonises data privacy laws across Europe.

The legislation is designed to protect EU citizens data privacy and to reshape the corporate approach to personal data privacy.

It covers **information** about the processing of personal data, and citizen's rights to **obtain access to** the personal data held about them.

What is covered

GDPR covers the processing by an **individual, a company or an organisation** of **personal data** relating to **individuals** in the EU.

Personal data is any information that relates to an **identified or identifiable living individual**.

Personal data that has been de-identified, encrypted or **pseudonymised** but can be used to re-identify a person remains **personal data.**

Who is covered

GDPR EU legislation is applicable to EU citizens.

Once an EU citizen's personal data is processed by an organisation, the person becomes a data subject with a number of rights.

EU citizens can demand that incorrect, inaccurate or incomplete personal data is **corrected.**

EU citizens can demand that personal **data be erased** when it's no longer needed or if processing it is unlawful (the right to be forgotten).

What is personal data?

- Personally identifiable information (PII)
- Technically identifiable personal information when linked to an individual
- Employment related identifiable information
- Personality related identifiable information such as personality insights
- Sensitive personally identifiable information (SPI)e.g. ID, racial/ethnic origins
- Financial information, such as credit card, bank account
- Healthcare information such as patient records, health insurance details

Scope of GDPR data privacy

There are already regulations in place about data security. GDPR extends the scope to **data privacy**.

GDPR applies to data stored anywhere about EU citizens, not just the EU

Data residency is about the location of data and metadata, the movement of (meta)data across geographies and jurisdictions, and the protection of that (meta)data against unintended access and other location-related risks

What does this mean

In practice, GDPR EU legislation requires strong security measures to protect individual's information, both at rest in data stores and in transit across the networks and internet

This includes information that when aggregated could potentially present an identifiable personal profile e.g. device ID, IP address

Achieving compliance with the **EU General Data Protection Regulation (GDPR)** means extending the organisation's data security journey

Steps to achieve compliance

- Review all data collections holding personal information covered by GDPR, including cross border data transfer and international storage.
- Ensure all data collection activities inform end users about data usage, data privacy, and update consent to collect data appropriately
- Plan for making individuals' data accessible on request
- Ensure functionality is available to accede to personal data requests for private data held, and to purge data on request.
- Review currency of compliance with EU Article 29 Working Party Opinions and Recommendations
- Implement security logging, monitoring and incident management processes, technologies and workflows for suspected data breaches