



GDPR in 60 seconds



New Responsibilities For Businesses

The EU General Data Protection Regulation comes into force on 25 May 2018 and will standardise data protection regulation across the European Economic Area.

Designed to govern how organisations treat personal information, putting individuals firmly in control of the way their data is used.

The overarching principles require the processing of personal data to be:

- Fair and lawful
- For specified purpose
- Adequate and relevant
- Accurate and up to date
- Retained for no longer than necessary
- Subject to rights of individuals

Key drivers are privacy, security, accuracy and accountability, which must be embedded into every aspect of your business.

Compliance is required by every organisation, regardless of size and location that holds personal information on data subjects, as consumers or employees, in the EU as well as organisations outside of Europe that process data on individuals within the EU.

You must determine and document the valid lawful basis for processing each piece of personal data, against six bases:

- Consent with positive Opt-in
- Contractual Obligations
- Legal Obligations
- Vital Interest
- Public Task Legitimate Interests
- Special Category Data
- Criminal Offence Data

N.B. We recommend that you check the ICO website (or relevant supervisory body) for the most up to date GDPR guidance.

More Information

If you are interested in learning how Maximizer CRM can help with your ongoing data management and GDPR compliance please contact us by email: gdpr@maximizer.co.uk

New Rights For Customers

The GDPR provides the following rights for individuals:

- The right to elect to be informed about how their data will be used.
- The right to access their personal data and supplementary information and verify the lawfulness of the processing.
- The right to have personal data rectified if inaccurate or incomplete.
- The right to erasure or 'to be forgotten' via requests for the deletion or removal of personal data if there is no compelling reason for continued processing.
- The right to 'block' or suppress processing of personal data with just enough information retained about the individual to ensure restriction request continues to be respected.
- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- The right to object under certain criteria.
- Rights in relation to automated decision making and profiling.

Non-Compliance and Data Breach Risks

There are stringent penalties for non-compliance with potential fines of up to 4% of annual global turnover or €20 Million (whichever is greater).

Failure to report certain types of data breach are open to potential fines of €10,000,000 or 2% of your global turnover.

In reality, such fines will continue to be a last resort by governing bodies, with a host of other tools available to help organisations comply including warnings, reprimands and corrective orders.

Be prepared to open both your business reputation and finance security to risk and impact.