



GDPR OVERVIEW

General Data Protection Regulation (GDPR) will go into effect on 25 May, 2018 across the European Union. Additionally, its 'extra territorial effect' means that companies outside the EU must also comply if they process personal data about people in the EU. Both personal data and processing have very broad definitions, so it's important to understand this from a GDPR perspective.

GDPR requires that data is:

1. Lawfully, fairly, and transparently processed
2. Collected for specified, explicit, and legitimate purposes
3. Adequate, relevant, and limited to what is necessary
4. Accurate and kept up-to-date
5. Kept in a form which permits identification for no longer than necessary
6. Processed securely

GDPR also requires that the controller of the data can demonstrate compliance.

The regulation also provides individuals' rights (with some restrictions) including:

1. The right to be informed
2. The right of access
3. The right of rectification
4. The right of erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

There are additional provisions for consent by a child and the processing of special categories of personal data including:

1. Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership
2. The processing of genetic data, biometric data, data concerning health or data about a person's sex life or sexual orientation
3. Data relating to convictions and offences

Data Protection Officer (DPO)

Under GDPR, data processors and data controllers must appoint a data protection officer if, as a core activity, they carry out large-scale, systematic monitoring of individuals or large-scale processing of special categories of data. The "EU Article 29 Working Party" guidance is that:

- Unless it is obvious that an organisation is not required to designate a DPO, you should document the internal analysis carried out to determine if you need to appoint one
- The DPO be located within the EU to ensure they are accessible



Current Status

There are a number of missing pieces in law, guidance, and industry standards that will be required before anyone can be truly ready for GDPR. M3 Global Research remains engaged with and actively tracking progress on these issues and will adjust its plans as the regulatory environment continues to evolve. For example:

- The “Data Protection Bill”, which will set out how the UK will apply the derogations available under GDPR, as well as various other measures, is still working its way through the UK parliament. Other countries in the EU are at various stages with their respective legislation.
- The UK regulator for GDPR, the Information Commissioners Office (ICO), has yet to issue their guidance on many important aspects of GDPR.
- Conversations between the MRS/EphMRA and the ICO regarding some important topics that impact our industry continue
- Consensus on how Adverse Event reporting will be possible under GDPR is starting to emerge, although, conversations between BHBIA and ABPI continue and many practicalities are yet to be addressed

M3 Global Research’s GDPR Readiness



M3 Global Research has been preparing for GDPR for a long time. This has been greatly assisted by our historic compliance focus:

- We were the first healthcare market research company to be ISO 27001 certified
- We were the first healthcare professional panel to be ISO 26362 certified
- We have an annual PricewaterhouseCoopers best practices and technology audit
- We are certified under the EU-US Privacy Shield and Swiss-US Privacy Shield and have Model Clause Contracts in place to allow our US operations to safely process EU data
- We have an experienced DPO in place to ensure GDPR compliance

Our GDPR team continues to refine our preparedness in conjunction with industry experts so that we can continue to provide our clients with industry leading data quality whilst adhering to all appropriate laws and regulations.