Fair Data™

General Data Protection Regulation Compliance Timeline

Get Ready Now

The General Data Protection Regulation (GDPR) comes into force from May 2018 and signals a new era for data protection in the digital world.

Organisations that monitor, store or analyse data will face more onerous obligations to comply, so it is essential to act now as failure to do so could attract significant fines.

The GDPR Compliance Timeline below shows exactly what needs to be achieved, when, in order to comply by 2018.

Fair Data is an accreditation trust mark for data protection that will take you much of the way towards GDPR compliance. Visit Fair Data to find out more, and keep up to date with GDPR developments on Twitter @fairdata.

Phase 1 — Phase 2 — Phase 3 — Phase 4

The Market Research Society 15 Northburgh Street, London EC1V OJR
Tel: +44 (0)20 7566 1874 Email: fairdata@mrs.org.uk

August to December 2016

Raise awareness and gather information

Your first steps should be to raise awareness of the GDPR within your organisation, gain consensus on the approach you will take, gather information on your current practices and prepare a project plan.

- **Inform decision-makers on the impact of the GDPR. Get consensus on its importance and approach.**

- **Conduct an information audit to fully understand your personal data use and processing.**

  - Ask the following questions:

    - Where is personal data stored?
    - How secure is it?
    - Who has control?
    - Is it shared?
    - Do you hold data of non-UK EU residents?
    - Is data transferred across borders or outside the EEA?

  - Identify personal data flows from EU to UK – these will need new adequate safeguard measures if the UK ends up outside the EEA (after its EU exit).
  - Identify activities that involve processing of data subjects in EU Member States as these will fall fully within the GDPR.
  - Who is responsible for data loss? This can be used to create a template for maintaining internal records of data processing required under the GDPR.

- **Understand the legal grounds on which you currently collect and use data. In particular, examine how consent and legitimate interests are used as the basis for processing personal data and document these.**

- **Review your IT systems and procedures.**

  - **Can your IT systems and organisational processes cope technically with new individual rights in a timely manner?**
  - **Think about subject access requests, data portability, right to be forgotten, recording objections or withdrawal from processing, and deletion of information.**

- **Review staffing requirements for data protection compliance.**

January to May 2017

Plan and prioritise

Phase 2

In phase two you should be prioritising key areas within your plan, appointing a Data Protection Officer and identifying areas with the highest risk and biggest potential impact.

- **Recruit and appoint a Data Protection Officer (DPO) – It will be mandatory for some organisations but in any event will be useful in most for developing and ensuring compliance.**

  - What is a DPO? The DPO should understand your business so they can assess key areas of privacy risks. The DPO is required to act independently and report to the highest level of management, so think about where the role will fit within the organisational structure. Note that this position can be outsourced to a competent firm or individual, which is an option that smaller organisations may wish to consider.

- **Focus on accountability of the organisation for data privacy - build a comprehensive privacy compliance programme and structure.**

- **Prioritise compliance activity and remedial measures based on areas with highest risk and most significant impact.**

  - Priority areas will include understanding the legal basis for processing and the new more specific requirements on getting consent right; processing of sensitive personal data; compatibility of systems with new rights such as data portability; and shorter time frames for subject access requests.

- Conduct Data Protection Impact Assessments (DPIA) for riskier activities –

- This includes identifying the need for a DPIA,
- Controllers will be required to perform a DPIA where the processing of personal data (particularly when using new technologies) is likely to result in a high risk to the rights and freedoms of individuals. DPIAs will particularly be required in cases of (i) an evaluation of personal aspects based on automated data processing including profiling; (ii) processing on a large scale of special categories of data; or (iii) systematic monitoring of a publicly accessible area.
- Describe the information flows and understanding where your data subjects are located. Identify any privacy risks and then identify and evaluate the privacy solutions. You can then sign off and record the privacy assessment outcomes and integrate the the outcomes into any project plan. It is important to consult with internal and external stakeholders as needed throughout the process.

- **Review and strengthen technical and security measures, specifically the use of encryption techniques.**

- **Prepare for data breach notifications:**

  - Set up internal procedures/strategy for data breach identification; establish the process for notification to the Information Commissioner's Office (ICO) and affected individuals; explore what "risk" to individuals means; build in effective ways of detecting breaches.

June to December 2017
Implement changes

Phase 3

Next steps are about implementing change: the priorities should be revising, updating and publishing your processes, policies and contracts.

- Integrate privacy by design and default – collect the minimum amount of information and consider privacy from inception of the product, service or project. Make sure you engage with the product teams early on.
- Review and update privacy policies and notices - improve the transparency and legibility of all public facing documents and involve copywriters to ensure they are user-friendly; consider innovative and creative ways of communicating information.
- Review and audit commissioning supply chain and update contracts.
    - Review and revise legacy contracts to consider mandatory terms; negotiate on apportionment of liability; consider adequacy of mechanisms for cross-border transfers, i.e. contracts with cloud providers. Controllers need to review selection criteria for processors and update contracts; Processors need to understand new obligations and assess impact.

January to May 2018
Embed change, train and re-train

Phase 4

In the last few months, the focus is on making sure changes are embedded within your organisation and your people are trained. Keep up-to-date with GDPR and UK plans for data protection reforms through Fair Data @fairdata.

- Implement the appropriate processes and policies in order to embed culture change and be able to demonstrate compliance with all obligations under the GDPR - including training for staff across the organisation
- Understand how codes and certifications can help with compliance on security, data transfers.[5]

25 May 2018
are you ready?

If your organisation has followed Steps 1 to 4 you will be compliant with Data Protection best practice both in the UK and Europe.

To show your customers and stakeholders that you uphold the highest standards of data protection, become a Fair Data company. The Fair Data accreditation enables you to demonstrate best practice. Find out more.

Call or email us to find out exactly how we can help on +44 (0)20 7566 1874 or fairdata@mrs.org.uk

MRS™

Fair Data is a quality process standard developed by the Market Research Society (MRS)