

GDPR Compliance Timeline

PHASE 1

Raise Awareness, Gather Information (2016-2017)

- Inform board members of the impact that the GDPR will have on your business.
- Conduct an information audit and record how you collect, store and use personal data.
- Verify that your legal grounds for processing personal data are legitimate.
- Review IT systems and procedures as well as staffing requirements for data protection compliance.

PHASE 2

Plan and Prioritise Compliance Efforts (January to May 2017)

- Recruit and appoint a data protection officer (not necessary for all organisations).
- Develop a comprehensive privacy compliance programme that holds you accountable.
- Prioritise personal data compliance activities throughout your organisation.
- Conduct a data protection impact assessment.
- Identify your riskiest data processing activities and strengthen your protection.
- Establish procedures to identify data breaches as well as to inform the ICO and affected individuals.

PHASE 3

Implement Changes (June 2017 to January 2018)

- Integrate privacy data by design and default into each of your processes.
- Review and update privacy policies and notices.
- Review and audit legacy contracts.

PHASE 4

Embed Change, Train and Retrain (January to May 2018)

- Provide GDPR training for your entire organisation that includes:
 - How to be compliant
 - How to recognise and identify a data breach
 - How to report a data breach
- Consider earning applicable codes and certifications, which can help with compliance on security and data transfers.

PHASE 5

Monitor, Review and Revise (Ongoing)

- Monitor your GDPR compliance efforts.
- Reassess whether your efforts are still effective. If not, make changes.
- Provide annual GDPR training for your organisation.