

Druces LLP - GDPR Compliance - You're too late...maybe!

Everyone who deals with personal data has to be compliant with the General Data Protection Regulation by 25 May 2018. There is a lot to do and it's difficult to know where to start.

In order to help you to get ready, Druces LLP has put together a GDPR compliance project plan and timeline to help organisations make sure they will not be breaking the law after next May. This sets out the major steps required and how long they could take. If you start now then you can be compliant in time; if you don't then you will run the risk of having to spend a lot more to get ready or you will just not be compliant.

If you have any questions about this plan, or any other GDPR issue, our data privacy team would be delighted to hear from you. Please contact Christopher Evans, Druces LLP on c.evans@druces.com

Task Name	Description	Duration (days)
Decision-makers	Build support with high-level managers to secure resources and budget. Establish cross-function compliance team.	25
Appoint DPO	Appoint Data Protection Officer to oversee compliance strategy.	25
Legal framework	Understand GDPR requirements and differences with current regime.	25
Data audit	Perform data audit, classify data by type and risk, determine legal grounds for processing.	45
Gap analysis	Review IT systems, procedures, cybersecurity and supply chain relationships to check compliance.	45
Risk assessment	Identify risks and prioritise remedial measures in areas of most significant risk and impact.	25
New solutions	Assess whether new solutions or software required; seek quotations from suppliers and conduct due diligence.	25
Supply chain contracts	Renegotiate supply chain contracts to deal with liability and cross-border data transfers.	150
Data breaches	Set up internal procedures to identify and deal with data breaches.	25
Update documents	Update privacy policies, notices and other public documents.	25
Establish Insurance	Contact insurance broker and arrange underwriting. Communicate terms of policy to management.	25
Training	Deliver training to ensure employees understand their compliance obligations.	25
Testing	Carry out a pilot test of new systems and procedures and make any necessary adjustments.	25
Monitor	Monitor effectiveness of systems and procedures. Keep up to date with GDPR guidance and refresh staff training.	130

