

The new EU General Data Protection Regulations (GDPR) is already law, with an enforcement date of 25 May 2018. By then, all businesses will need to be fully compliant or face heavy fines, which means you need to make the necessary changes now.

GDPR replaces the existing Data Protection Act and changes the way personal data can be handled, with consumers having increased rights over the way their data is collected, maintained and shared. It aims to create a uniformity of rules across the EU and improve the customer experience.

At present, the onus is on the consumer to opt out, which may involve 'unticking a box' or stating clearly they do not want their data to be collected and used. Under the new regulations, the onus is on the data collector to gain permission to gather personal data, and to provide total transparency as to how it will be used.



**To give you the essential facts about GDPR, here is a useful 10-step guide:**

1. You must be GDPR compliant before 25 May 2018 or face heavy fines
2. Personal data will need to be processed transparently, lawfully, for specific purposes, and be kept up-to-date.
3. The definition of personal data is wide reaching. Final official guidance on the interpretation of this definition from the Information Commissioner's Office is still awaited, but we believe it will include business email addresses that can identify an individual
4. The vast majority of business to business, and business to consumer marketing will be affected
5. Individuals will have the right to see what data you hold about them and request it is removed
6. Information held about individuals must be held 'with consent' or 'for a legitimate purpose'
7. 'With consent' means the individual will have given explicit permission for you to hold and use their data
8. Your processes will need to evolve to provide 'freely given opt ins' rather than existing 'opt outs'
9. You can only hold data relating to activities you have received permission to use it for
10. You must be able to DOCUMENT, PROVE & DEMONSTRATE you are doing all the above – and more!

There will be tough penalties for data abuse, and any company not complying with the new GDPR could face fines of up to 4% of their annual turnover. Please also be aware that the Privacy and Electronic Communications Regulations (PECR), which sit alongside the Data Protection Act give people specific rights in relation to electronic communications, such as marketing calls, emails, texts, faxes and cookies.

We will update you on GDPR as its implications become clearer. We do also recommend you view the Information Commissioner's Office website, [ico.org.uk](https://ico.org.uk), on a regular basis to keep fully up to date on how GDPR could affect you.

**Sources:**

Preparing for the GDPR – Information Commissioner' Office: <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/><https://nilehq.com/gdpr-download/>  
<http://www.eugdpr.org/>  
<https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/>  
Also, for internal info: Willis Towers Watson Networks: Marketing Insider Letter: Practice Group Special Edition