

# Subscribe to the facts

**Senior managers across the UK are reacting to the new data regulations coming into force on 25th May, many of them implementing new policies that could damage their business in a bid to comply with the General Data Protection Regulation (GDPR). Andrew Scott, managing director of Insight Data says companies need to get the real facts**

Scare mongering and profiteering among so-called consultants is causing many within marketing, IT and HR departments to panic, with some drawing comparisons to the Year 2000 computer crisis where some pundits predicted worldwide computing disaster and planes falling out of the sky.

The new General Data Protection Regulation is a good thing; it is designed to give individuals greater rights and control over how their data is used. The recent Facebook and Cambridge Analytica scandal highlights why this has become so important.

The GDPR sets new standards in how personal data is collected, stored and processed. The regulation replaces the existing Data Protection Act (DPA) which was written before major data processors such as Facebook, Google or Apple had such large-scale global dominance.

GDPR is about data transparency and governance. Companies who already operate good data practices will find it relatively easy to comply, while others will need to evaluate their business processes and make changes.

‘Consent’ is only one way to comply

There is significant misinformation surrounding the GDPR particularly relating to ‘consent’. Under the GDPR consent must be ‘unambiguous, informed and freely given’. However, there are six legal grounds for processing data with consent being just one of them. For many companies ‘legitimate interest’ will be the basis of compliance particularly for marketing communications.

Understanding the wider context of the GDPR highlights a risk-based approach to how data is collected, stored and processed. A company processing confidential personal medical or financial data, or data that includes children or highly sensitive information represents a much higher risk than a B2B supplier that holds the names of its customers, for example.

With this in mind, companies are advised to carry out a data protection impact assessment (DPIA) which considers how its data is collected, stored and processed and assesses the risks involved.

Organisations that choose to adopt ‘legitimate interest’ as the legal grounds for processing personal data should also conduct a legitimate interest assessment.

Businesses will need to demonstrate that they have taken all reasonable steps to comply with the GDPR including: clearly document the personal data they hold, how and when it was sourced, how it will be used, how it is updated and who will have access to it.

Demonstrate the lawful basis for processing personal data.

Have freely available privacy policies that are fair and easy to understand and explain what personal data is held, how it was sourced, for what purpose and the legal basis for processing data.

Recognise the rights of individuals to know what



**Andrew Scott**

personal data is held and why, and respect their demand to correct, restrict or remove their data.

Have procedures in place to detect and report on a data breach, such as a computer hack, theft of data by an employee or other breach.

Assign someone to take overall responsibility for data protection and compliance.

While the GDPR governs how data is collected, stored and processed, how data is used for marketing purposes is mainly covered under PECR, the Privacy and Electronic Communications Regulations which has sat alongside the Data Protection Act and was introduced in 2003 to regulate direct marketing, clamping down on nuisance phone calls and spam.

While the Data Protection Act is replaced by the GDPR on 25th May, PECR has not, in fact, changed.

It is not surprising that so many marketers are confused. The GDPR outlines how data must be processed, but the rules governing how the data is actually used for marketing – PECR – have not been updated. A new version of PECR, the ePrivacy Regulation is currently being formulated and should be introduced in 2019. □

[www.insightdata.co.uk](http://www.insightdata.co.uk)

**Insight Data has published guides and information on the GDPR on its website and recommends all companies follow the advice of the Information Commissioners Office (ICO). Insight has been tracking the GDPR since its first proposal and began updating its prospect database to meet the requirements of the regulation back in 2016. For more information visit [www.insightdata.co.uk](http://www.insightdata.co.uk)**