Key Features of GDPR

(General Data Protection Regulation)

Introduction

The European Union (EU) has changed its data protection rules. The changes are now law and they will go live across the EU on **25 May 2018**. These new rules are called the General Data Protection Regulation (GDPR) and apply across the board from public authorities to small and medium-sized businesses.

What we need to do

The GDPR is a long document but here are some things we'll need to do:

1. Make sure we only process data fairly and lawfully.
2. Make sure we tell people properly when we collect their personal data and get their consent.
3. Make sure we only hold data which we need.
4. Keep the data we hold accurate and up-to date.
5. Keep data secure.
6. Respect people's right to opt out at any time.
7. Do data protection impact assessments when doing something new.
8. Make sure we're ready to deal with the new rights created by GDPR – like the rights for people to see the data we hold on them, to move it, to correct it and to have it deleted.
9. Make sure we destroy data when we don't need it any more – and that we do this securely.
10. Make sure we only share data with people we trust – and even then have a proper written agreement in place.
11. Deal with problems like potential data breaches quickly.
12. Remember: GDPR applies to hard copies and electronic data.

Let your data protection officer (or CEO if you don't have one) know as soon as possible if you think there's been a data breach – this applies if its electronic data (like the email system) or manual data (like papers in a filing cabinet).

Bigger penalties

Remember there are bigger penalties under the new rules. From 2018 for some infringements a maximum fine of €20 million or 4% of the global annual turnover of a business (whichever is the greater) can be imposed, with likely higher reputational damage resulting too. This is the big stick for data protection compliance, but, getting it right will avoid major headaches.