Countdown to the General Data Protection Regulation

We are now on the final countdown to the General Data Protection Regulation (GDPR), which will apply in the UK from 25 May 2018.

Mairead O'Reilly
Consultant
T: 020 7551 7782
m.oreilly@bwbllp.com

Mairead advises charities and social enterprises on a range of commercial and charity law issues. She has particular expertise in the areas of data protection and information law.

Mairead O'Reilly looks at the practical implications for charities and social enterprises

The GDPR has been one of the most anxiously awaited pieces of legislation of recent years. While it will undoubtedly introduce a number of changes to data protection practices, in most cases the GDPR should not radically alter how you approach data protection compliance. Many of the core principles will remain the same, so for organisations that currently follow sound data protection practices, getting ready for the GDPR will not be an insurmountable task!

Below are what we think are the vital practical steps which charities and social enterprises should be taking now and over the next nine months.

1. Get ready to work differently with suppliers which are processing personal data on your behalf (i.e. data processors), such as payroll providers, professional fundraisers and software providers. Agreements with these companies will need to be reviewed to make sure they are 'GDPR ready'. This needs to happen now for contracts that will continue past 25 May 2018.
2. Where you rely on consent for any reason – whether to process a member's details or to send email fundraising, check that it meets the new higher threshold set out under the GDPR. Existing consents obtained under the Data Protection Act will need to be brought to a GDPR standard in time for 25 May 2018.
3. Put in place mechanisms to ensure that you can record and comply with any withdrawal of consent by individuals.
4. Review your privacy statements. These will need to be much more comprehensive and detailed under the GDPR.
5. Introduce policies and train staff on the new rights that individuals will have under the GDPR, so that you are ready to comply with requests as soon as they come in. These will include the complex 'right to be forgotten'.
6. Determine whether you will need to employ a Data Protection Officer under the GDPR. This will depend on whether you are a 'public authority', and on the type of processing that you are carrying out.
7. After May 2018 you will no longer be required to maintain an annual registration with the ICO. Instead you will need to prepare templates for keeping new internal records of processing. You will also need to prepare to carry out Privacy Impact Assessments for any 'high risk' profiling.

'Many of the core principles will remain the same, so for organisations that currently follow sound data protection practices, getting ready for the GDPR will not be an insurmountable task'

8. Update your data security policies and train staff on the new obligation to report data security breaches within 72 hours where they present a risk to individuals, which is discussed in more detail in the article on the opposite page.
9. If you are an international organisation based outside the EU and engage with supporters or customers in the EU, you may need to appoint a representative in the EU.
10. There will be a sharp increase in the fines which the ICO can issue for data protection breaches (up to €20 million). This needs to be reflected in your organisation's data protection risk assessments.

Find out more
BWB is running a series of seminars setting out practical tips for organisations getting ready for GDPR compliance. For more information see here: http://www.bwbllp.com/events/all/2017/11/23/gdpr-event-session