GDPR WHAT YOU NEED TO KNOW

THE **GENERAL DATA PROTECTION REGULATION** IS A NEW LAW WHICH WILL REPLACE THE CURRENT DATA PROTECTION ACT

Institute of Fundraising

Small Charities Coalition

THE BASICS FOR CHARITIES

WHEN DO WE HAVE TO BE READY?

MAY 2018
25

DON'T LEAVE IT TOO LATE

By 25th May 2018 you'll need to be ready to meet the requirements - don't leave it too late, start thinking through and implementing changes now!

WHAT'S NEW?

'EVOLUTION NOT **REVOLUTION'**

GDPR is the biggest overhaul of data protection legislation for over 25 years – it introduces new requirements for how organisations process personal data. But, many of the requirements already apply under the DPA – as the ICO says, GDPR is an 'evolution not revolution'.

DOES THIS APPLY TO CHARITIES?

GDPR APPLIES TO ALL SECTORS

YES - GDPR applies to all sectors and organisations processing personal data, including charities. That includes (but is not limited to) data you hold and process on your supporters, service users, volunteers, and staff.

FOCUS ON FUNDRAISING

WHAT DO FUNDRAISERS NEED TO KNOW?

GDPR DOESN'T STOP YOU FUNDRAISING

Fundraisers need to make sure that all processing of personal data of supporters is done fairly and lawfully, respecting the privacy rights and choices of individuals.

WHAT IS PERSONAL DATA?

MORE THAN JUST NAME AND CONTACT DETAILS

Under GDPR, the definition of personal data has been broadened and includes any information relating to an identified or identifiable natural personal - not just their name and contact details.

CAN I SEND DIRECT MARKETING TO INDIVIDUALS?

CONSENT OR LEGITIMATE INTEREST

YES - but you need a lawful basis to process an individual's personal data to send direct marketing. 'Consent' is a lawful basis to send direct marketing, and so is 'legitimate interest' (for non-electronic communications). For more info, see IoF's guidance, GDPR Essentials

THE LEGAL BIT

WHO REGULATES DATA PROTECTION?

ico.

The Information Commissioner's Office regulates data protection law in the UK and provides guidance.

www.ico.org.uk

Make sure you know the rules and are following them, GDPR isn't optional!

WHAT COUNTS AS A BREACH?

72H

A personal data breach means a "breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data." Controllers must report a data breach to the ICO no later than **72 hours** after being aware of the breach (unless there is a low risk to the individual's rights).

WHAT ARE THE CONSEQUENCES OF NON-COMPLIANCE?

€20M

- Fines of up to **€20 million,** or **4%** of annual global revenue (whichever is greater)
- Damage to reputation
- The risk of lawsuits

For more information and resources go to **www.institute-of-fundraising.org.uk/GDPR**