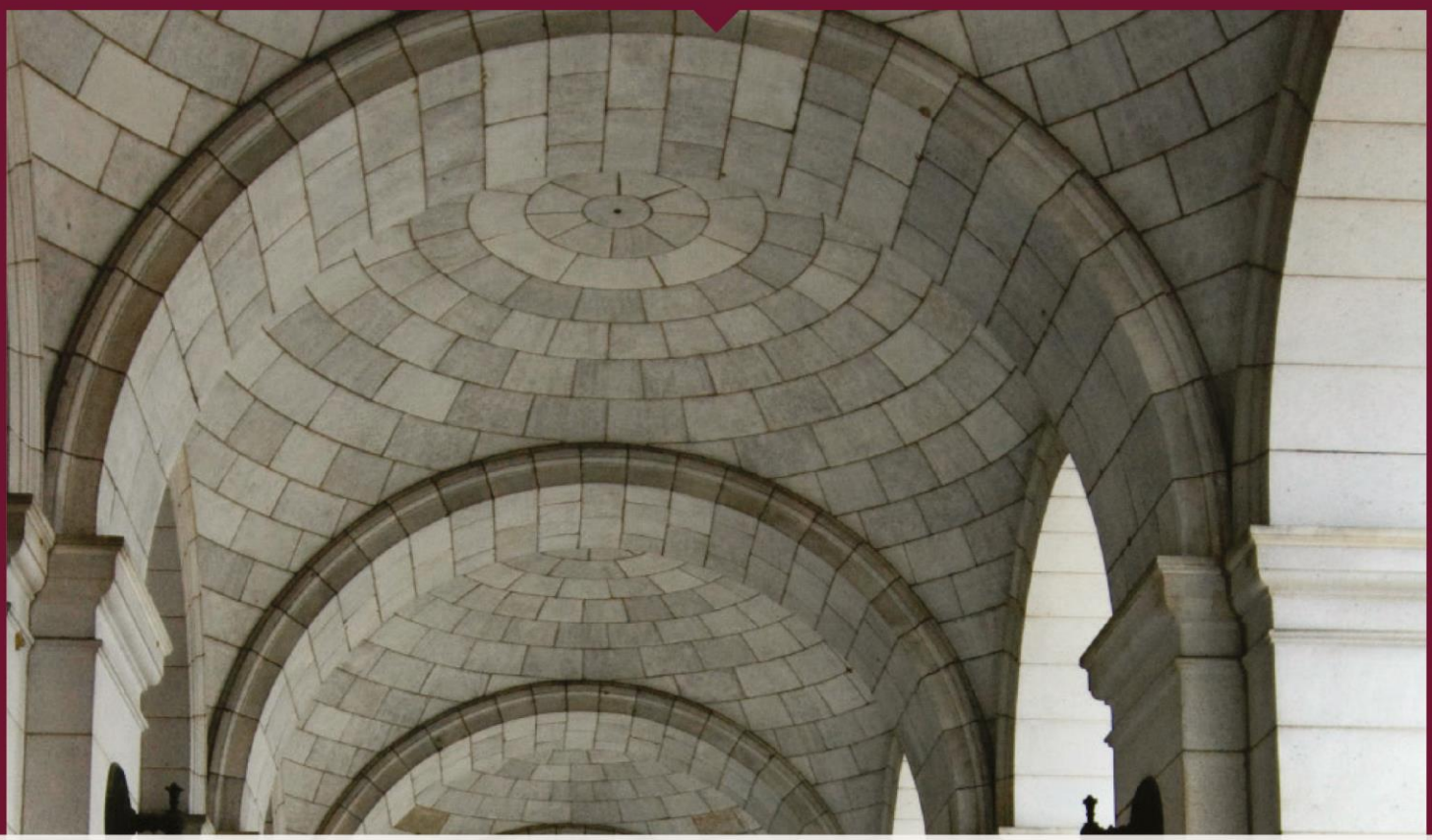

General Data Protection Regulation

What does it mean for community energy organisations?

Background

The EU laws which founded the Data Protection Act 1998 (**DPA**) – now the cornerstone of the UK's current personal data protection regime – were written well before Mark Zuckerberg was out of short trousers, let alone contemplating his Facebook empire. 25 May 2018 will see a huge shift in the regulation of data protection across the EU.

This is the date from which EU organisations will have to comply with the General Data Protection Regulation (**GDPR**). GDPR is designed to respond to the significant advances in information technology, and the fundamental changes to the ways in which we communicate and share information, which have occurred since the mid-1990s. In addition, it is designed to create a more harmonised approach to data protection laws across the EU, being directly applicable without the need for national implementation.

GDPR

Many of the core concepts under the existing regime (the Data Protection Directive (**DPD**)) will remain unchanged. For example, the concepts of personal data, data controllers (a person who determines the purposes for, and the manner in, which any personal data is processed), and data processors (a person who processes personal data on behalf, and under the instruction, of their data controller), are broadly similar in both DPD and GDPR. However, GDPR will introduce several new concepts and approaches, the most significant of which are as follows.

- Non-EU data controllers and data processors will be subject to GDPR if they either offer goods or services to individuals in the EU, irrespective of whether payment is received; or monitor individuals' behaviour insofar as their behaviour takes place within the EU. This means that many non-EU organisations that were not required to comply with DPD will be required to comply with GDPR.

- GDPR requires a very high standard of consent from an individual when relied upon by community energy organisations to legally process their personal data. This must be given by a clear affirmative action establishing a freely given, specific, informed and unambiguous consent. When the processing of personal data has multiple purposes, an individual should give their consent to each of the processing purposes. An individual has the right to withdraw their consent at any time.

- Community energy organisations will be required to implement data protection by design (e.g. when creating new products or services) and by default (e.g. data minimisation), both at the time of the determination of the means for processing and at the time of the processing itself. Community energy organisations will also be required to perform impact assessments before carrying out any processing (e.g. via new technologies) that is likely to result in a high risk to individuals.

- Instead of registering with their National Data Protection Authority (**NDPA**) (in the UK, the Information Commissioner's Office – (**ICO**)), community energy organisations must maintain detailed documentation recording their processing

activities as specified by GDPR. In addition, in certain circumstances controllers or processors will be required to appoint a data protection officer.

- Individuals will have the right to request that community energy organisations delete their personal data in certain circumstances (e.g. their data is no longer necessary for the purpose for which it was originally collected). Individuals have a new right to obtain a copy of their personal data from the data controller in a readable and usable format, and in exercising this right individuals can request the information be transmitted directly from one controller to another, where technically feasible.

- Community energy organisations must notify the ICO of all data breaches without undue delay and where feasible within 72 hours, unless the data breach is unlikely to result in a risk to the individuals concerned. If the breach is likely to result in high risk to individuals, GDPR requires organisations to inform those individuals "without undue delay" as well.

- GDPR introduces direct compliance obligations for processors, meaning they can be subject to fines. It will significantly increase the maximum fines that NDPAs will be able to impose on data controllers and data processors. The maximum fines are set on a two-tiered basis as follows:

    - For violations relating to data processor contracts, data protection officers, data protection by design and default, internal record keeping and data breach notification – the greater of 2 per cent of annual worldwide turnover of the preceding financial year, or 10 million euros.

    - For violations relating to individuals' rights, conditions for consent, international data transfers and breaches of the data protection principles – the greater of 4 per cent of annual worldwide turnover of the preceding financial year, or 20 million euros.

How Wrigleys can help

Wrigleys have produced a series of podcasts covering various aspects of GDPR. For access to our podcasts, or if you would like more detailed information on any of the points covered above, please visit our website.