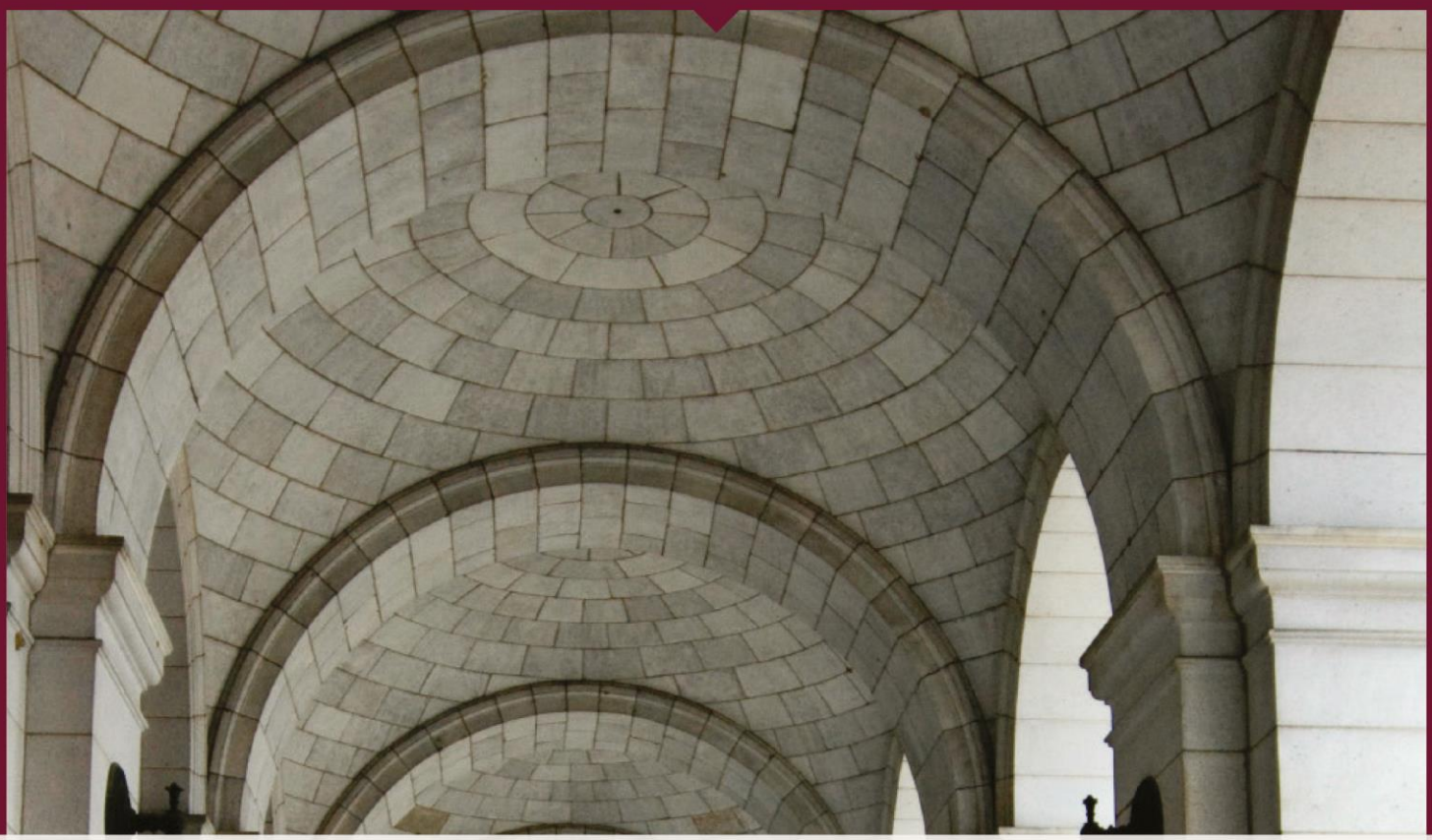

General Data Protection Regulation

What should community energy organisations be doing to prepare?

The implementation date of 25 May 2018 for the General Data Protection Regulation (GDPR) is fast approaching. With compliance required from day one, it is important that community energy organisations are taking steps now to ensure they comply with the new regime.

Getting ready for GDPR

GDPR should be high on the agenda at any director or management meetings between now and May (and indeed afterwards). We have identified three key steps that organisations should be taking to prepare for GDPR:

- Understand what personal data you hold and process (data mapping)
- Understand the lawful basis for holding and processing each type of personal data (lawful basis analysis)
- Implement any changes to your policies, processes and procedures to ensure compliance (implementation)

Data mapping

A data mapping exercise is useful to identify the personal data held by a community energy organisation, and the types of processing carried out in relation to that data. It can help work out the information coming in and going out of an organisation, as well as what happens to the data in the interim.

Wrigleys have produced a data mapping questionnaire which community energy organisations can use to assist them with their data mapping exercise. It can be found here.

Lawful basis analysis

Data processing must be within one of the prescribed legal bases under GDPR. These are listed below and there are conditions to the availability of each basis which must be satisfied:

- The individual has given ***consent*** to the processing for one or more specific purposes;
- Processing is necessary for ***entering into or performing a contract*** with the individual;
- Processing is necessary to comply with the organisation's ***legal obligations***;
- Processing is necessary to protect the ***vital interest*** of the individual;
- Processing is necessary for the performance of ***a task carried out in the public interest*** or in the exercise of ***official authority*** vested in the organisation or a third party to whom the data is disclosed; or

- Processing is necessary for the purposes of ***legitimate interests*** pursued by the organisation or a third party, except where such interests are overridden by the rights and freedoms of the individual.

Community energy organisations need to understand which lawful basis is available to them for each processing activity and, if more than one basis is available, which basis is most appropriate, given the circumstances of the organisation and the individual(s) to whom the data relates.

Implementation

Compliance with GDPR includes compliance with six data processing principles, and should be recorded in a data protection policy. Personal data should be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
- kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data is processed; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The data mapping questionnaire and lawful basis analysis exercise will help community energy organisations to determine what steps they then need to take to ensure compliance with GDPR. However, we have set out below certain steps that organisations are likely to need to take:

- **Privacy notices**

  At the point when personal data is obtained from an individual, they must at the same time be provided with certain information, including the purpose of and legal basis for the processing of their data. This can be done in the form of a privacy notice. Updated privacy notices should also be sent to all individuals for whom the community energy organisation holds personal data before GDPR comes into effect.

- **Consent**

  Special categories of data can only be processed with the individual's consent, such as data relating to their health. If a community energy organisation holds data falling into one of these special categories, it needs to decide whether to destroy, return or retain the data. If retaining the data, it must have the explicit written consent of the relevant individual to do so.

- **Individuals' rights**

  Individuals about whom personal data is held have rights in relation to that data, including a right of access and a right to erasure. The individual has to be informed of these rights, and personnel within community energy organisations should make sure that they have had sufficient training to understand what these rights are, when they can be enforced, and any associated time limits.

- **Contracts**

  Personal data can often be passed to third parties (e.g. payroll providers). Community energy organisations will need to make sure that the third parties that they work with are also GDPR compliant, by putting in place (or amending existing) data protection agreements with third parties.

- **Written records**

  Community energy organisations will have to maintain a written record of the processing activities they undertake, as well as those they have responsibility for but do not undertake themselves. The record will have to be available to the Information Commissioner's Office (ICO) on request.

- **Ensuring data security**

  Appropriate technical and organisational measures should be implemented ahead of time to ensure a level of security appropriate to the risk. This might include encryption of data, restoration in the event of a physical or technical incident and ongoing assessment of security measures. Community energy organisations should review their existing measures and determine where new measures need to be introduced.

- **Reporting protocol**

  Where there is a personal data breach, community energy organisations should notify these to the ICO without delay and, where possible, within 72 hours of becoming aware of the breach. In some circumstances, the breach must also be communicated to the individual without delay. Data protection policies will need updating to cover an organisation's protocol in the event of a data breach. Appropriate reporting and communication channels will also need to be put in place.

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.