

**The procedures have changed since the 25<sup>th</sup> May 2018. This is an explanation of how it now works.**

### **A Procedure**

- **Fee:** an organisation will not be able to charge for complying with a request unless the request is 'manifestly unfounded or excessive'. The data controller may charge a reasonable administrative-cost fee if further copies are requested.
- **Excessive requests:** if a request is 'manifestly unfounded or excessive' data controllers can charge a fee or refuse to respond but will need to be able to provide evidence of how the conclusion that the request is manifestly unfounded or excessive was reached.
- **Electronic access:** it must be possible to make requests electronically (e.g. by email). Where a request is made electronically, the information should be provided in a commonly-used electronic form, unless otherwise requested by the individual.
- **Content of response:** the request should allow the individual to know what information is held about them and what processing is being carried out. In responding to a request, data controllers may need to provide further information such as the relevant data retention period and the right to have inaccurate data corrected.
- **Time to respond:** the data controller must respond to these requests within a month, with a possibility to extend this period for particularly complex requests. Under the DPA, the response time is 40 days.
- **Right to withhold:** data controllers can withhold personal data if disclosing it would 'adversely affect the rights and freedoms of others'. This is reflective of the current position under the DPA. The recitals to the GDPR note that this could extend to intellectual property rights and trade secrets. Member States may introduce further examples such as legal privilege.

### **B What will the impact be on the organisation?**

- Organisations will have to deal with requests more quickly, as well as providing additional information.

- Individuals already have a right to access their personal data through a SAR. However, it will generally be free to make those requests and individuals will be entitled to receive the information in an electronic format.

If an organisation handles a large number of SARs, the impact of the changes could be considerable. Therefore, taking steps to organise the approach to SARs will help organisations to comply with the GDPR.

## **C What actions should you take to prepare?**

- Update your procedures and plan how you will handle SARs and provide any additional information within the new timescales.
- Develop template response letters to ensure that all elements of a response to a SAR under the GDPR are being complied with.
- Assess your organisation's ability to quickly isolate data pertaining to a specific individual and to provide data in compliance with the GDPR's format obligations.
- Ensure that employees are trained to quickly recognise and respond appropriately to SARs.
- Consider putting a 'data subject access portal' in place allowing an individual to access their information easily online and minimising cost for the data controller dealing with the SAR.