## 10 steps to becoming GDPR compliant

**How to approach GDPR:** GDPR is principles based (Article 5 GDPR) and takes a risk-based approach to data protection. This allows practices to decide for themselves what steps are appropriate and proportionate to comply with GDPR, meaning that the approach large practices need to take to get ready for GDPR is likely to be different to the approach smaller firms and sole-practitioners need to take.

1. **Awareness** – Ensure that key people in the organisation are aware that the law is changing on **25 May 2018**. It is important to appreciate the potential impact of GDPR, identify areas that could cause compliance problems and the resources required to address any concerns.

   Staff should be provided with relevant training so that they understand how GDPR may impact their day to day working and what additional support and resources they may need from the organisation to be compliant.

   It is also important to talk to any third parties that you share personal data with. This may include IT and case management providers to ensure they are ready for the changes and to determine any steps needed to update systems and processes.

2. **Information** – Practices should consider documenting i) what personal data the practice holds, ii) where it came from, and iii) who it is shared with. An information audit may need to be carried out to achieve this.

   Consideration should be given to implementing systems to verify individuals' ages and to obtain parental or guardian consent for any processing activity in relation to children.

3. **Demonstrating compliance** – Practices should be able to show that they are compliant with GDPR and a record of any data processing activities should be maintained.

   A data protection policy, a data breach notification procedure, data protection impact assessments and consent forms will also help to demonstrate compliance. The scale of the policies and procedures should be appropriate to the size and complexity of the practice.

4. **Communicating privacy information** – Practices must be open and transparent about the reasons they are collecting personal data and what they intend to do with it. The most common way to do this is to provide the information in a privacy notice.

   Existing privacy notice should be reviewed and updated to ensure individuals are provided with the appropriate information, for example, the lawful basis for processing the data, data retention periods and individuals' right to complain to the Information Commissioner's Office (ICO) if they think there is a problem in the way their data is being handled.

5. **Individual's rights** – Procedures should be in place to protect all of the individual's rights including dealing with a request to delete or transfer personal data.

6. **Subject access requests** – A review of the procedure for dealing with subject access requests (SARs) should be carried out to take into account the new rules about providing information to individuals:

   a. In most cases, practices cannot charge for complying with a request for information.

   b. Practices will have a month to comply, rather than the current 40 days.

   c. Practices can refuse or charge for requests that are 'manifestly unfounded or excessive'.

d. If a request is refused, the individual must be informed why and that they have the right to complain to the ICO. This must be done without undue delay and at the latest, within a month.

7. **Lawful basis for processing personal data** – The lawful basis for collecting any personal data should be documented for each processing activity to help comply with GDPR's accountability requirements.

8. **Consent** – Practices should review how they seek, record and manage consent. Consent must be freely given, specific, informed and unambiguous.

   Existing consents obtained under the DPA 1998 do not automatically need updating if they meet the GDPR standard of being 'specific, granular, clear, prominent, not automatically opted-in, properly documented and easily withdrawn'.

9. **Data breaches** – Procedures should be in place to detect, report and investigate a personal data breach without undue delay.

   Any personal data breach which could impact an individual or cause harm must be reported to the ICO without undue delay, and no later than 72 hours after detection. If the breach is likely to result in a high risk of adversely affecting individuals' rights, practices must also inform those individuals without undue delay.

10. **Data Protection Officer (DPO)** – GDPR sets out criteria when a DPO must be appointed. Most CLC regulated practices are unlikely to come within these criteria although practices may still wish to appoint a DPO.

April 2018