

What is GDPR?

GDPR stands for General Data Protection Regulations and is a new piece of legislation that will supersede the Data Protection Act. It will not only apply to the UK and EU; it covers anywhere in the world in which data about EU citizens is processed.

The GDPR is similar to the Data Protection Act (DPA) 1998 (which the practice already complies with), but strengthens many of the DPA's principles.

The main changes are:

- Practices must comply with subject access requests.
- Where we need your consent to process data, this consent must be freely given, specific, informed and unambiguous.
- There are new, special protections for patient data.
- The Information Commissioner's Office must be notified within 72 hours of a data breach.
- Higher fines for data breaches – up to 20 million euros.