NHS
Building a Digital Ready Workforce

# GDPR for GDPs

## Guidance for compliance with the General Data Protection Regulation in Dental Practice

## Key Facts

- There is an expectation that practices are compliant with the General Data Protection Regulation (GDPR) from 25th May 2018
- Your practice data protection policy will need to be modified to comply with certain changes under the GDPR
- New information registers and logs are required to record and report on data flows, information assets, to monitor compliance, to provide a record of staff training, for breach reporting and to review data quality
- Readily accessible privacy statements are necessary for patients and staff to inform them about how you store and use their data
- Your practice will need to register as a data controller with the Information Commissioner's Office (ICO) and there may be circumstances where associate dentists will be required to do so also

PLEASE NOTE

This document is an interpretation of the GDPR written by Dr Francis Clough. It is for guidance only and does not constitute legal or business advice. For more information about the GDPR please visit the Information Commissioner's Office (ICO) website: www.ico.org.uk.

## What is the GDPR?

The General Data Protection Regulation (GDPR) is the new, incoming European regulation for data protection that will supercede the Data Protection Act 1998 (DPA).

## When does it come into force?

May 25th 2018

## What does it mean?

The regulation aims to give citizens more control over their personal data. This means data of any kind, including that which is in digital format, how it will be processed (by a data processor) and who it will be controlled by (data controller).

## What is a data controller?

A data controller is an organisation or individual that collects personal data, determines the purposes and means of processing the data. In relation to dental practice this will include the dental practice and all employees therein as well as local authorities, commissioners and local area teams where applicable.

## What is a data processor?

The organisation that is responsible for processing personal data on behalf of a data controller. In dental practice this includes any individual, organisation or company that is contracted to process the information collected by the practice. This will include practice management software companies, referral management services or other bodies with whom there exists a written contract to process data only on instructions from the data controller.

## What is data protection?

Personal data is information relating to an identifiable living individual. Whenever personal data is processed, collected, recorded, stored or disposed of it must be done within the terms of the Data Protection Act 1998 (DPA).
Data protection relates to the discipline of processing and storing personal data appropriately, fairly and lawfully and within the anticipated remit of purposes for which it was obtained.

## Why should you care?

Under the GDPR, data protection becomes the responsibility of everyone (dentists, nurses and all admin staff) involved in collecting, handling and accessing data; it is no longer just the clinician in charge of a patient's care.
Under the GDPR, serious data breaches may result in heavy fines being imposed.
Organisations stand to be fined up to 4% of their annual turnover, which will significantly compromise the stability of companies, for mishandling personal data.
The maximum fine threshold increases from £500,000 to £17 million.

# Data Protection Compliance under the GDPR

| Requirements | Compliant? |
|---|---|
| Designated Data Protection Officer (DPO) | |
| Copy of the privacy notice that is available for members of public and staff members | |
| Information audit of data flows | |
| Confirmation of ICO registration/notification | |
| Information asset register | |
| Lawful basis for processing personal data | |
| Practice consent policy | |
| Detail of arrangements with respect to the following patients' rights and actions to support them:<br>- The right to be informed;<br>- The right of access;<br>- The right to rectification;<br>- The right to erasure;<br>- The right to restrict processing;<br>- The right to data portability;<br>- The right to object;<br>- The right not to be subject of automated decision-making | |
| Records management policy | |
| Compliance measures and monitoring processes | |
| Staff training log and planned at regular intervals | |
| Written contracts with data processors | |
| Information asset risk assessment | |
| Breach reporting policy | |
| Data protection impact assessment | |
| Data quality checks and data quality reviews of systems | |