GDPR FAQs

The United Chiropractic Association are not legally qualified GDPR experts. We are providing the enclosed information as a service to our members. Please note some of the regulations are open to interpretation, and clarity for some aspects will only be obtained long after 25th May 2018.

In addition, some of the finer detail is still being clarified by the EU and as such may change the intention, meaning or interpretation of any part of the regulations.

If you need clarification on any aspect of GDPR you should seek specialist advice. The United Chiropractic Association, or its representatives, cannot accept any liability for any loss or damage you may incur as a result of this material.

- **What is the GDPR?**
  The General Data Protection Regulation is a new, European-wide law that replaces the Data Protection Act 1998 in the UK. It places greater obligations on how organisations handle personal data. It comes into effect on 25 May 2018.

- **What information does the GDPR apply to?**
  The GDPR applies to 'personal data', which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. You can find more detail HERE

- **Does the GDPR only apply to EU organisations?**
  The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

- **How can I prepare?**
  You can find the latest ICO guidance on the new legislation HERE
  The ICO has also created a package of tools aimed at small and micro businesses:

  Getting Ready For The GDPR – a practical self-assessment tool
  12 Steps Checklist
  Dedicated Advice Line For Small Organisations

  The GDPR is an evolution of the existing law. If you are already complying with the terms of the Data Protection Act 1998, and have an effective data governance programme in place, then you are already well on the way to being ready for the GDPR.

- **But I'm only a small business…does GDPR still apply to me?**
  Yes. You have to comply with the GDPR (regardless of your size) if you process personal data.

If you have less than 250 employees you only need to document processing activities that:

- are not occasional; or
- could result in a risk to the rights and freedoms of individuals; or
- involve the processing of special categories of data or criminal conviction and offence data.

See HERE for more information on documentation.

- **Do I need to appoint a Data Protection Officer (DPO)?**
  Any organisation can choose to appoint a DPO and although it is mandatory for organisations processing a large scale of special categories of personal data, GDPR does not actually define what large scale is – so the ICO cannot enforce this part of the regulation.
  Examples of large scale processing can be found HERE

  The European Parliament has requested an amendment to GDPR to quantify large scale:
  "Finally, Parliament adds that a DPO should be mandatory for all enterprises that process 'Special categories' of data, including information such as health data or religious and political beliefs. The Commission text requires any enterprise over 250 employees, while the Parliament text calls for those processing the personal data of over 5000 data subjects in any 12-month period."

  If you are satisfied that this role is not necessary for your clinic, or you wish to appoint a staff member and are satisfied this will not lead to a conflict of interest (so not directly involved in processing the data), then document this decision and store in your compliance manual.

- **What if I want to appoint a DPO even though I may not need to?**
  If you employ a practice manager who does not, as part of their role, directly input patient data then arguably there would be no conflict of interest so they could be the DPO. Note that they have to be suitably knowledgeable about GDPR.

  A family member (who does not process the data) may be a willing volunteer! As with the practice manager they would need to be suitably knowledgeable about GDPR.

  Outsourcing may be an option for you. Various organisations are offering this services and it may be a cost effective way to ensure you maintain compliance.

  Minimise your data. Rather than keep patient treatment notes "forever", destroy them after the minimum period. The less data you hold, the lower the risks and the need for a DPO may be less significant.

- **Do I have to destroy personal data after 2 years, or after 8 years as stated by GCC?**
  Firstly, there is a difference between personal data and medical records.

Personal data should not be kept for longer than is necessary for the purpose you obtained it for. Click HERE for more info.
Personal data is things like name, address, telephone number, email - and can come from things like screenings, booked appointments that were never attended and emailed queries.

With regards to medical records it is a legal and professional requirement that these are kept for 8 years – please see page 2 of the GCC's Guidance on Confidentiality.

As you must comply with this you will not be considered as having kept the information for longer than necessary.

If a patient requests that you destroy their records before the 8 year period ends, simply advise them that, by law, you must keep them for a 8 year period.

- **Do x-rays count as personal data?**
  X-rays formulate part of the medical record NOT personal data. As such you are still able to charge up to £50 for a copy of these.

- **What are Subject Access Requests?**
  A Subject Access Request (or SAR) enables individuals to find out what personal data you hold about them, why you hold it and who you disclose it to.
  Please see HERE for more info.

- **Do I have to be registered with the ICO?**
  If you process personal information you must register with the ICO.

  Not sure if you need to register?
  Take the ICO's quick self-assessment to find out.