GDPR (General Data Protection Regulation) comes into law in the UK on 25 May 2018

This is a very brief, unofficial guide. You are urged to consult the ICO (Information Commissioner's Office) https://ico.org.uk/ or https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/ for more detailed information.

Principles

Personal data must be:

- **Processed lawfully, fairly and transparently in relation to the data subject.**
  Transparency: Tell the subject what data processing will be done. Fair: What is processed must match up with how it has been described. Lawful: Processing must meet the tests described in GDPR [article 5, clause 1(a)]
- **Collected for specified, explicit and legitimate purposes.**
  Personal data can only be obtained for "specified, explicit and legitimate purposes" [article 5, clause 1(b)]. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.
- **Adequate, relevant and limited to what is necessary.**
  Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". [article 5, clause 1(c)] i.e. No more than the minimum amount of data should be kept for specific processing.
- **Accurate, and kept up to date**.
  Data must be "accurate and where necessary kept up to date" [article 5, clause 1(d)] Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data.
- **Storage limitations**
  Kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which it is processed. Data no longer required should be removed.
- **Integrity and confidentiality**
  Processed in a manner that ensures adequate security of the personal data using appropriate technical or organisational measures including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

If you hold data on clients, in any form, whether on paper or electronically, you are a data processor and you must abide by the GDPR. "Data Processing" means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.

Steps to take NOW (taken from the ICO website, italics from the author) – some of these may not all be applicable to you or your organisation:

1) **Awareness**

Make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2) **Information you hold**

Document what personal data you hold, where it came from and who you share it with *(it is unlikely that in our context you share any personal data with anyone, except verbally in supervision for example)*. You may need to organise an information audit.

3) Communicating Privacy Information

Review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation. Privacy Notice: You need to communicate to people the lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data. This must be provided in concise, easy to understand and clear language.

4) Individuals' rights

Check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format. The following are individuals' rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The right not to be subject to automated decision-making including profiling

5) Subject Access Requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information. Important aspects of this rule:

- In most cases you will not be able to charge for complying with a request.
- You will have one month to comply.
- You can charge for or refuse requests that are manifestly unfounded or excessive.
- If you refuse a request, you must tell the individual why and that they have the right to complain to the ICO and to a judicial remedy. This must be done without delay, within one month.

6) Lawful basis for processing personal data

Identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7) Consent

Review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8) Children *(under 16)*

Start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9) Data Breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach. You only have to report breaches to the ICO where it is likely to result in a risk to the rights and freedoms of individuals, if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. If a breach needs to be reported, this must be done within 72 hours of discovery of the breach.

10) Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11) Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer. *It is highly unlikely that in our context this is not necessary.*

12) International

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help ou do this. *It is highly unlikely that in our context this is not necessary.*

Personal data identifying data subjects

This is data relating to living individuals who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of the data controller. It need not be confidential data:

- Names.
- Addresses and other location data.
- IP addresses and other online identifiers (email address).
- Telephone numbers.
- Job titles.
- Salary details.
- Medical details.
- Dates of birth.

Special care is needed in some cases, if you record:

- Racial or ethnic origin.
- Religious or philosophical beliefs.
- Health data.
- Sexual or sexual orientation data.

Pseudonymisation

Means the processing of personal data in a way where it can no longer be matched to a specific data subject without additional information, and provided such additional information is kept separately and securely. Pseudonymous data is NOT exempt from the GDPR.

Fines for non-compliance

These are very high, and can be result from:

- Breaching the obligations imposed by a monitoring or certification body.
- Failing to notify in the event of a data or security breach.
- Not having the necessary technical/organisational measures in place to protect data.
- Not keeping proper written records of processing activities.

Some of the implications of this are:

Consent

This must be:

- Freely given.
- Specific and informed.
- Specific for each purpose and activity of the processing operation.
- Be clear about how the individual can withdraw their consent at any time.
- Unambiguous.

The data processor must ensure that they have clear and unambiguous consent from the individual on whom they hold information. This is best done by having the client sign a contract including their consent. The record of consent should specify how and when consent was given. This should also make clear your data privacy policies.

Note that failure to opt-out is not consent.

Children (under 16):

- You must have parental consent for processing data of an individual under the age of 16. Where court proceedings are involved, there may be special clauses to this which would need investigating. NB: according to the BACP there is "no requirement for parental consent for data processing related to counselling" – this needs further checking which has not been completed at the time or writing this document. (BACP ref: https://www.bacp.co.uk/bacp-journals/counselling-at-work/january-2018/an-upgrade-for-data-privacy/, 20/02/2018)

Security procedures

You need to know what your procedures are to protect the data you hold.

Destruction of personal data

You must understand how you destroy personal data.

Right to access

Any information held about a person belongs to that person, and they a right to view all information that you hold about them.

Breach notification

If at any time you have reason to believe that the data you hold on an individual has been seen by another individual, you MUST: inform the client, your professional body, and the ICO within 72 hours of the breach occurring.

Right to be forgotten

Your clients have the right to ask you to destroy any data that you hold on them. This may well take precedence over any requirements outlined in Codes of Professional Practice which stipulate periods for which client notes should be kept.

How long should I keep data?

There is not set period, so you need to decide what is appropriate for a particular client.

Useful information on the UKCP website.

Held at https://www.psychotherapy.org.uk/registers-standards/gdpr/

Receiving a request for your notes

From time to time, therapists are asked by the police or solicitors (for example) to assist them in a case by asking them to hand over their notes. The general principles remain the same. Remember that you must have consent from the individual to pass on the information and even if you have this, you may want to carry out a redaction exercise. Note that the Police do not have authority to demand you hand over your notes. Only a Court of Law can oblige you to do this. So even if a client has given their consent to the Police, you must excercise your judgement as to whether you think it is in their best interests to do so. Remember, the data protection regulations are aimed at protecting the rights of individuals over information that concerns them.

Some suggestions for therapists

- Familiarise yourself with the new GDPR regulations – look at the ICO website.
- Make sure you are trained by bone fida trainer / consultant / organisation.
- Check your client contract. It must be clear, unambiguous, and clearly state what you will do with data provided by your client, and state that your client can request deletion at any time, and can complain to the ICO if they think you have breached data rules. In simple terms, tell your clients what you are doing with their data. This means that if you are planning to use anything they disclose for the purposes of any written work like supervised practice report, case study, oral exam, make this clear to your client and have their signature for explicit permission to do so.
- Example from BACP of some areas that need to be included in a client contract :
    - State who is the Data Controller and whether they are registered with the ICO (if you are in private practice this is likely to be yourself)
    - Set out the purposes and legal basis for processing client personal data
    - Clarify the circumstances in which data may be shared with other agencies (e.g. immediate risk of substantial harm to self or others; or under a legal requirement, e.g. terrorism, drug money laundering; or via court order for disclosure)
    - State how long client records are kept, before being securely destroyed
    - Explain client rights under data protection law, i.e. to access a copy and explanation of their personal data to request correction or erasure, in certain circumstances to request limiting or ceasing data processing, where applicable to compensation for substantial damage or distress caused by data processing, where applicable
- As far as possible, keep succinct notes of client work, but always keep notes, however brief.
- Do not make copies of client notes, either electronically or physically. Do not carry written notes on your person unless absolutely necessary.
- Take great care that all written notes are held in a locked environment.

- Be sure that you know where your notes are kept. This may seem obvious, but in particular with electronic notes it is very important that you know where your information is held.
- Keep a backup of your electronic information, being sure that the backup is securely encrypted, not just password protected. However, always use passwords on any device and make sure you use strong passwords. I suggest that you do note use 'Cloud' based backup services. If you do, then you need to ensure that they comply with ICO regulations.
- Do not keep notes or backups on small memory sticks – these are very easy to lose, and this would constitute a very serious breach. If you do, make absolutely sure that your disk is encrypted.
- Do not disclose notes to any party, including the police, without an explicit, signed waiver from your client. Only a Court of Law can oblige you to disclose client notes.
- Don't panic! As long as you can show you did your best to comply, you will be OK.
- Consider whether you are holding information that you don't need, and if so delete it. Only retain data if you know you need to.
- Do not send audio files of client sessions by email or any other internet based file sharing system.

Document prepared by John Baxendale, Wealden Psychology Institute, Crowborough.
john@wealdeninstitute.co.uk