**General Data Protection Regulation (GDPR)**

**Guidance for HG therapists**

**Important Changes to Data Protection Regulation**

*First published: May 2018
Last updated: May 2019*

On **25th May 2018** the data protection regulations were significantly strengthened when the **General Data Protection Regulation (GDPR)** became law throughout the EU, including the UK and Republic of Ireland. The subsequent **Data Protection Act 2018** is the UK's implementation of the (GDPR). [**http://www.legislation.gov.uk/ukpga/2018/12/part/1/enacted**](http://www.legislation.gov.uk/ukpga/2018/12/part/1/enacted)

**GDPR: 8 Principles of Data Protection:**

1. Obtain and process information fairly
2. Keep it only for one or more specified, explicit and lawful purposes
3. Use and disclose it only in ways compatible with these purposes
4. Keep it safe and secure
5. Keep it accurate, complete and up to date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it for no longer than is necessary for the purpose or purposes
8. Provide individuals with a copy of their personal data free of charge, on request.

**What does this mean for therapists?**

Importantly, the legislation tightens up the rules around how people’s personal information is obtained and the use that can be made of it. In practice, this means that clients must be given sufficient information about how their personal data will be used so that they are able to give their fully informed, ‘explicit’, consent to its collection and retention. The following **Privacy Notice**, which has been added to the customisable [**Information for Clients sheets**](https://www.hgi.org.uk/general-data-protection-regulation-gdpr#download-documents)and reflected in the [**HGI Confidentiality Agreement forms**](https://www.hgi.org.uk/general-data-protection-regulation-gdpr#download-documents), aims to cover the above requirement:

"**Your personal information** will be kept in accordance with the Data Protection legislation on the basis that you have given your consent to information about you being held by the therapist, which means that they will:

* use your contact details only to get in touch with you about matters relating to your therapy, such as appointments and to provide helpful information, where appropriate, unless you have given your explicit consent for the therapist to contact you for other purposes.
* retain notes of your treatment for a period of 7 years, in accordance with professional requirements and will take steps to ensure the security of the record.
* not share your personal information with other individuals or organisations, except where they have reason to believe you or others to be at risk, or where there is a legal duty to disclose it, or as otherwise specified, if applicable.
* provide you with free access to the information they hold about you, should you wish.”

**Notes**

1. **NB:**With regard to the first bullet point above, it is important that you do not use clients’ contact details for marketing, advertising or promotional purposes, unless you have their explicit (written) consent to do so.
2. With regard to the issue of the sharing personal information (third bullet point above), it is important that where a client is referred to you by an agency, they are made aware at the outset of any requirement for you to inform the agency of the therapy outcome together with related details as appropriate. Clauses covering this aspect have been added to the HGI Confidentiality Agreement forms. (Where not applicable, these should be deleted from the forms.)
3. Members are advised to display the above privacy notice, or an equivalent statement, on their websites.

**Right to be informed**

The GDPR ‘Right to be informed’ provision stipulates that clients must be informed of the identity and contact details of the data controller, i.e. in our case the therapist. Also, they must be informed about the controller’s representative, i.e. the HGI.

The pre-existing customisable HGI Information for Clients sheet covers part of the above in that it requires therapists to add their name and contact details and includes information about the HGI. However, in light of the GDPR, the document has been expanded to include information on the use and retention of personal data (see below) and the basis for lawful processing of that information, which in the case of the HGI is **explicit consent**.

Note: It will be clear from the above that if you currently adhere to existing data protection legislation and ethical principles, by obtaining informed/explicit consent and respecting the confidentiality of client information, you will already be going a long way towards meeting the new requirements. However, there is more…

**Children**

In the UK, only children aged 13 or over are able to provide their own consent to the provision of their personal data (and also to treatment). Note: 13 is the age stipulated in the UK Data Protection Act 2018 ([**http://www.legislation.gov.uk/ukpga/2018/12/part/1/enacted**](http://www.legislation.gov.uk/ukpga/2018/12/part/1/enacted)).

In the Republic of Ireland the age of consent is 16, whilst in Germany, it has been set at 16.

A consent/confidentiality agreement form for the use of parents/guardians of children under the age of 13 has been produced and can be downloaded from the Members Area of the HGI website ([**click here to view**](https://www.hgi.org.uk/general-data-protection-regulation-gdpr#download-documents)).

**Notes:**

1. Whilst the UK Data Protection Act 2018, states the UK age of consent as 13 years in the UK, Clauses 9(a) and 9(b) of the Act qualify this feature:
	* **Clause 9(a)** sets the age of consent for processing at 13 years. The Explanatory Notes point out that this is in line with the age set by Facebook, Whatsapp, and Instagram. It also means that children aged 13 and above would not need parental consent when accessing educational websites and resources to complete homework.
	* **Clause 9(b)** states that the reference to “information society services” does not include “preventative or counselling services”.

Clause 9(b) indicates that a child under the age of 13 can access counselling without parental consent, if they wish to do so. The most likely context in which this might occur would be in schools which employ a counsellor, or in relation to an organisation, such as the NSPCC, where a child does not wish their parent(s) to know. In the much less likely event of a child under 13 requesting counselling from a private practitioner, the practitioner can proceed, although they will need to be fully aware of their duties under child protection/safeguarding requirements, as for instance set out in the [**HGI Policy and Guidelines for Therapists Work with Children**](https://www.hgi.org.uk/private-practice/essential-information/hgi-policy-and-guidelines-therapists-work-children).

Where a parent requests counselling for a child under the age of 13, therapists should make use of the parental consent form that is available in the Members Area – see above.

1. If a young person claiming to be 13 or over requests treatment without the knowledge of a parent, the therapist, if in doubt, should take steps to verify their age. Further information on the GDPR requirements in relation to children can be viewed via the ICO website: [**https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/**](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/)

For Republic of Ireland: [**http://www.gdprandyou.ie**](http://gdprandyou.ie/)

**Referral of clients by other agencies**

If you take referrals from an agency, it is important that you seek assurance from the organisation concerned that it meets the GDPR requirements in relation to the lawful processing of clients’ personal information, e.g. that they have obtained their informed/ explicit consent. If applicable, you must also make clear that it is not acceptable for the agency to send clients’ personal information by email, unless it has been encrypted or fully anonymised. Otherwise, personal information should be sent by post (to be signed for) or dictated over the phone.

**Online services**

If you provide therapy via a digital platform, you must still obtain the explicit consent of clients and provide them with clear information about how their personal information will be used, etc, as described above.

**Data Controllers**

Under the current data protection regulations, everyone who holds the personal information of clients in either paper or digital form, is classed as a ‘**data controller**’. However, only those who hold, and/or transmit personal data digitally, are required to register as data controllers with the Information Commissioner’s Office (ICO – see below).

If you use an electronic device (computer, mobile phone) to communicate with clients, you should register as a data controller with the Information Commissioners Office as soon as possible, since such devices store contact details automatically. Information on how to register can be found on the ICO website at [**https://ico.org.uk/for-organisations/register/**](https://ico.org.uk/for-organisations/register/)

Further information about data controllers can be downloaded from the ICO website at [**https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf**](https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf)

For Republic of Ireland: [**https://www.dataprotection.ie/**](https://www.dataprotection.ie/)

**Security of Data**

In brief, if you keep client data on a computer or smartphone, etc, the device should be password protected and sensitive files encrypted. Where ‘data subjects’ (clients in our case), can be identified from the content, it is highly inadvisable to transmit sensitive personal information electronically. Paper records must be stored securely, eg in a lockable cabinet. Note: To reduce the of loss or damage in the event of a flood, it is advisable to store paper records above floor level. *Please see the Additional Information section of this document for further advice on data security.*

A Practical guide to IT security can be downloaded from the ICO website: [**https://ico.org.uk/media/for-organisations/documents/1575/it\_security\_practical\_guide.pdf**](https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf)

**Data breaches**

Under the new legislation, if a personal data breach occurs, the data controller is required to notify the ICO no later than 72 hours after becoming aware of it, unless the breach is unlikely to result in harm to ‘rights and freedoms’ of the client and/or other parties. (Where the notification is not made within 72 hours, reasons for the delay must be provided.)

If the breach is likely to result in harm to a client or other party, the data controller must notify them and if necessary provide information on how they can protect themselves from the consequences of the breach.

All breaches must be documented and a record maintained by the data controller.

Failure to take the prescribed action in respect of data breaches can result in fines. If in doubt, please seek guidance from the ICO [**https://ico.org.uk/**](https://ico.org.uk/) or the HGI Registration and Professional Standards Committee (RPSC), which can be contacted via the HG office.

**Right to the erasure of data**

GDPR strengthens individuals’ right to have their data erased, or ‘to be forgotten’ by organisations. However, in the case of health-related records there is an exemption. This what the ICO says:

**You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:**

* to exercise the right of freedom of expression and information;
* to comply with a legal obligation for the performance of a public interest task or exercise of official authority;
* for public health purposes in the public interest;
* archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
* the exercise or defence of legal claims. *Note: This last clause is particularly relevant to the retention of case notes.*

For further information see: [**https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/**](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/)

With regard to the length of time client records should be held, professional indemnity insurers stipulate in the region of 7 years. In this regard, Balens’ website includes the following:

**GDPR and Record Keeping**

Currently our policy wording notes:

The records shall be kept for at least 7 years following the last occasion on which treatment was given. In the case of treatment to minors, it is advisable that records should be kept or at least 7 years after they reach the age of majority (18). *Record Keeping - Condition 14 c, on page 35*

It is likely that our policy wording following GDPR will keep in line with the above, however we are waiting for further clarification from our Insurance partners regarding this. We will ensure that we write to all clients as soon as we have had confirmation and in good time for them to comply with GDPR.

For further information, go to Balens’ website at [**http://www.balens.co.uk/news/gdpr-2018.aspx**](http://www.balens.co.uk/news/gdpr-2018.aspx)

Members who are with other insurers are advised to check their websites for relevant information, or contact them direct.

**Pragmatic Tracker**

The owners of the Pragmatic Tracker database have taken steps to ensure that the programme meets GDPR requirements.