Good Practice in Action Legal Resource 097

Update on Data Protection Legislation

Context

This resource is one of a suite prepared by BACP to enable members to engage with the current BACP *Ethical Framework for the Counselling Professions* in respect of the law.

Using the legal resources

The *Ethical Framework for the Counselling Professions* establishes a contractual commitment between BACP members and BACP. These legal resources are not contractually binding on members, but support good practice by offering general information on principles and policy applicable at the time of publication.

The legal resources should not be used to constitute legal advice in specific cases, nor are they sufficient on their own to resolve legal issues arising in practice. As practice issues and dilemmas arising from work with clients are often complex, we strongly recommend consulting your supervisor, and also, wherever necessary, a suitably qualified practitioner or lawyer. Some professional insurers will provide legal advice as part of their service.

Specific issues in practice will vary depending on clients, particular models of working, the context of the work and the kind of therapeutic intervention provided. Please be alert for any changes that may affect your practice, as organisations and agencies may change their practice and policies. References in this resource were up to date at the time of writing but there may be changes to the law, government departments, websites and web addresses, and it is important for you to keep informed of any changes that may affect your practice.

In this resource, the word 'therapist' is used to mean specifically counsellors and psychotherapists and 'therapy' to mean specifically counselling and psychotherapy.

The terms 'practitioner' and 'counselling related services' are used generically in a wider sense, to include the practice of counselling, psychotherapy, coaching and pastoral care.

The term 'Data Controller' refers to someone who determines the purpose & means by which personal data is processed. It is not always easy to ascertain who is acting as controller and who is acting as a processor but most therapists will be Data Controllers

The term Data Processor refers to a person or organisation that processes Personal Data on behalf of a Data Controller. This could include IT companies, record keeping companies, archivists etc

Current Data Protection Legislation

Under current data protection legislation, where sensitive personal client data are kept and stored electronically, no matter what the format, (so this may include clients' information on computers, laptops, mobile phones, discs, tapes, or any other forms of recordings etc.), registration as a 'data controller' is required under the Data Protection Act 1998 (see: https://ico.org.uk/for-organisations/register/self-assessment/ and subsidiary legislation. The Register is accessible and searchable on-line at www.ico.gov.uk. If unsure if this applies, take the 'Does registration apply to me?' test at www.ico.gov.uk

The New Data Protection Laws

New legislation, the European Union's *General Data Protection Regulations ('GDPR')* will come into force on 25th May 2018, and have direct effect in all European states. Despite Britain's impending exit from the European Union, a new Data Protection Bill has been brought before Parliament which will bring in the provisions of the GDPR as law within the UK.

Guidance is still being issued and updated by the ICO, see https://ico.org.uk/for-organisations/data-protection-reform/ .

Therapists are encouraged to check the website of the ICO at regular intervals for updates in the guidance, and the impact of the legal changes on our data processing procedures.

For the text of the GDPR, and key facts, also see https://www.eugdpr.org/eugdpr.org.html.

Key changes to the UK's data protection regime, following the GDPR will include:

- Consent – there is a much higher standard for consent. Anyone processing the personal data of another individual (the data subject) must ensure that the data subject's consent was a *freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."* Asking a data subject to tick a box agreeing to a general or vague statement will not be sufficient evidence of consent. In addition, you must make it easy for people to withdraw their consent and tell them how they can do this.
- Data Subjects have the right to be informed about how you are using or processing their personal data and should be provided with a 'fair processing notice' (typically given through a privacy notice) meaning all data controllers must provide more detailed information to data subjects about how their data will be processed, what it will be used for and who it will be shared with.
- Data breach notification – the Information Commissioner's Office (ICO) will have to be notified about any breaches which may pose a risk to the rights and freedoms of individuals.
- Fines – the ICO will be able to impose mammoth fines on organisations, up to the higher of 4% of worldwide annual turnover and EUR 20 million, depending on the nature, gravity and duration of the infringement.
- Data subjects' rights – these will be bolstered, with the right to be forgotten, to correct data which are wrong or to restrict certain processing, and the right for data subjects to ask for their personal data to be handed back or sent to another data controller (known as 'data portability'). Data subject access requests will have to be responded to, within a month and without a requirement to pay a fee, unless the request is 'manifestly unfounded or excessive'.
- Data protection officers – some data controllers and processors will be required to appoint data protection officers to oversee their data processing activities. There may be further changes, so practitioners are advised to check the Information Commissioner's website www.ico.gov.uk at regular intervals for updates on the operation of the GDPR and other legislation as it comes into force.
- under the GDPR there is no longer an obligation to register (i.e. notify) data processing with the Information Commissioner's Office. However, a provision in

the Digital Economy Act means it will remain a legal requirement for data controllers to pay the ICO a data protection fee.

- Contracts – Data Controllers will be required to have written contracts in place with any Data Processors appointed by them.

Sensitive Personal Data

In current data protection law, briefly, most of the information held by therapists will be regarded as 'sensitive personal data'. Sensitive personal data contain information about:

- Racial or ethnic origin
- Political opinions
- Religious beliefs or beliefs of a similar nature
- Trade union membership
- Physical or mental health condition
- Sex life
- Criminality, alleged or proven

The GDPR continues to define these categories of data as 'sensitive data' and adds to this list genetic data, and biometric data where processed to uniquely identify an individual.

The use of sensitive personal data already requires the client's explicit consent and will continue to do so. The client has to actively state that they are agreeing to a record being kept and used in the knowledge of the purpose(s) for which the record is being made, how it will be used and any limitations on confidentiality. This should be the routine practice of therapists who hold computerised records or who hold manual records in any form of an organised filing system.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing and the new Data Protection Bill sets out specific conditions providing lawful authority for processing it which mean that this type of data is dealt with in a very similar way to the special categories of data outlined above.

Children's Personal Data

The GDPR contains new provisions intended to enhance the protection of children's personal data. Where services are offered directly to a child, you must ensure that your privacy notice is written in a clear, plain way that a child will understand.

Processing Personal Data

As well as consent, there are other lawful grounds for processing personal data. These are:

1. Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
2. Processing is necessary for compliance with a legal obligation
3. Processing is necessary to protect the vital interests of a data subject or another person

4. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
5. Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

On most occasions, therapists will need to obtain the consent of a client to process that client's personal data but there may be occasions (for example to prevent harm to the client or someone else) when one of the above grounds will be required.

If the Data Protection legislation applies to any data in a therapist's possession, then:

1. That Personal data must be:
    a. Processed fairly and lawfully
    b. Obtained only for one or more specified and lawful purposes, and shall not be processed in any manner incompatible with that purpose or those purposes
    c. Adequate, relevant and not excessive
    d. Accurate and, where necessary, kept up to date
    e. Not be kept longer than necessary
2. The clients' rights must be respected.
3. You must take appropriate security measures to protect the personal data in your possession; and.
4. Personal data shall not be transferred outside the European Economic Area (All EU Member States plus Iceland, Liechtenstein and Norway).

Records may also be created and stored in written form e.g. on paper. If the records are in an organised filing system, i.e. an accessible format – kept in a neat and tidy order, which would make information in them logical and so easily located, even though the records may be protected by anonymity with links and codes etc., the Data Protection legislation will still apply to these handwritten or typed client records. For details see www.ico.gov.uk.

Rights of the Data Subject

Data Subjects already have rights in respect of their personal data and these will be enhanced by the GDPR. Included among these rights are:

1. The Right to Erasure

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

1. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
2. When the individual withdraws consent.
3. When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
4. The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
5. The personal data has to be erased in order to comply with a legal obligation.

6. The personal data is processed in relation to the offer of information society services to a child.

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

1. to exercise the right of freedom of expression and information;
2. to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
3. for public health purposes in the public interest;
4. archiving purposes in the public interest, scientific research historical research or statistical purposes; or
5. the exercise or defence of legal claims.

There are extra requirements when the request for erasure relates to children's personal data. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent.

2. The Right to Data Portability

This right allows a data subject to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer their data easily from one IT environment to another in a safe and secure way.

It applies when:

1. Data has been provided from an individual to a controller
2. Where processing is based on consent or for the performance of a contract, and
3. When processing is carried out by automated means.

If a therapist receives a request to transfer a data subject's personal data, he or she must provide the personal data in a structured, commonly used and machine readable form and the information must be provided free of charge.

If the individual requests it, you may be required to transmit the data directly to another organisation if this is technically feasible. However, you are not required to adopt or maintain processing systems that are technically compatible with other organisations.

If the personal data concerns more than one individual, you must consider whether providing the information would prejudice the rights of any other individual.

3. The Right of Access

The data protection legislation gives the subject of personal data a right to access to the information which is being held about them. This right is referred to as a 'subject access right' to all electronically stored records and to the data held about the client in structured manual files. The aim is to enable any citizens to know what information is being processed about them. A written request, proof of identity (if required) and (currently) payment of the prescribed fee entitles the data subject to be informed about what data are being processed, for what purpose, to whom they have been or may be disclosed, and to be provided with a copy of those data. This information should be provided within 40 days, and the release of records cannot be made conditional, e.g. on the client paying any outstanding fees. From the 25th May 2018, the time to respond will be reduced to one month and the obligation to pay a fee for the data will be abolished.

A client who considers that there is an inaccuracy in the record may ask for it to be corrected with the agreement of the therapist. If there is disagreement about what would be a correct record, it is good practice to include a record of the client's objections in the notes.

Any therapist who is concerned about the client's response to seeing their records may offer to be present and explain the records or to arrange for another suitably qualified person to be present. If the therapist is concerned that access to the notes would cause serious harm to the physical or mental health of the data subject and that access to the notes may constitute a health risk, it may be possible to refuse or defer access with the authorisation of the health professional who is currently or was most recently responsible for the clinical care of the person concerned (Data Protection (Subjects Access Modification) (Health) Order 2000 section 7) https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/. The legal presumption in favour of access to personal data makes this an exceptional provision that ought not to be sought or granted lightly.